Regulator constants of integral representations of finite groups

Alex Torzewski

Abstract

Let G be a finite group and p be a prime. We investigate isomorphism invariants of $\mathbb{Z}_p[G]$-lattices whose extension of scalars to $\mathbb{Q}_p$ is self-dual, called regulator constants. These were originally introduced by Dokchitser–Dokchitser in the context of elliptic curves. Regulator constants canonically yield a pairing between the space of Brauer relations for G and the subspace of the representation ring for which regulator constants are defined. For all G, we show that this pairing is never identically zero. For formal reasons, this pairing will, in general, have non-trivial kernel. But, if G has cyclic Sylow p-subgroups and we restrict to considering permutation lattices, then we show that the pairing is non-degenerate modulo the formal kernel. Using this we can show that, for certain groups, including dihedral groups of order $2p$ for p odd, the isomorphism class of any $\mathbb{Z}_p[G]$-lattice whose extension of scalars to $\mathbb{Q}_p$ is self-dual, is determined by its regulator constants, its extension of scalars to $\mathbb{Q}_p$, and a cohomological invariant of Yakovlev.

Contents

1 Introduction

Regulator constants are invariants of representations of a finite group introduced by Dokchitser–Dokchitser (see for example [DD09]). We shall briefly recall some of the basic properties of regulator constants (cf. Section 2.5).

Let G be a finite group. A Brauer relation in characteristic zero (resp. characteristic p) consists of a pair of G-sets for which the associated permutation modules over $\mathbb{Q}$ (resp. $\mathbb{F}_p$) are isomorphic. Characteristic zero (resp. p) relations form a free abelian group of finite rank, which we denote by $br_0(G)$ (resp. $br_p(G)$). All characteristic p relations are also characteristic zero relations so that $br_p(G) \subseteq br_0(G)$ (Lemma 2.7).

If $\mathcal{R}$ is a ring, then by an $\mathcal{R}[G]$-lattice we mean an $\mathcal{R}[G]$-module which is free of finite rank as an $\mathcal{R}$-module. We will be mainly interested in the case of $\mathcal{R} = \mathbb{Z}_p$, the p-adic integers, and $\mathcal{R} = \mathbb{Z}_{(p)}$, the localisation of $\mathbb{Z}$ at p. Let $\mathbb{Q}_p$ denote the field of p-adic numbers. We call a $\mathbb{Z}_p[G]$-lattice *rationally self-dual* if its extension of scalars to $\mathbb{Q}_p$ is self-dual. Each characteristic zero Brauer relation θ defines a regulator constant $C_\theta(-)$ which assigns to a rationally self-dual $\mathbb{Z}_p[G]$-lattice M an element $C_\theta(M) \in \mathbb{Q}_p^\times/(\mathbb{Z}_p^\times)^2$. As will be made precise later, $C_\theta(M)$ measures the relative covolumes of certain fixed subspaces corresponding to the G-sets defining θ (see Definition 2.25).

In several number theoretic contexts, regulator constants have been found to both coincide with naturally occurring objects and to be computationally accessible. For example, if $K/\mathbb{Q}$ is a Galois extension of number fields with $G = \mathrm{Gal}(K/\mathbb{Q})$, $E/\mathbb{Q}$ is an elliptic curve and $M = E(K)/E(K)_{\mathrm{tors}}$, the torsion-free quotient of the Mordell-Weil group of E, then the regulator constants of $M \otimes \mathbb{Z}_p$ are closely related to the elliptic regulator of E [DD09]. Similarly, if $M = \mathcal{O}_K^\times/\mu_K$ is the unit group of K modulo roots of unity, then the regulator constants of $M \otimes \mathbb{Z}_p$ are closely related to Dirichlet's unit group regulator [Bar12].

The applications of regulator constants are dependent on showing that regulator constants are good invariants of lattices. In this paper, we systematically investigate the strength of regulator constants as invariants of lattices.

Let $a(\mathbb{Z}_p[G])$ denote the representation ring of G over $\mathbb{Z}_p$. We write $a(\mathbb{Z}_p[G], \mathrm{sd})$ for the subring generated by $\mathbb{Z}_p[G]$-lattices which are rationally self-dual. Set $A(\mathbb{Z}_p[G]) = a(\mathbb{Z}_p[G]) \otimes_\mathbb{Z} \mathbb{Q}$, $A(\mathbb{Z}_p[G], \mathrm{sd}) = a(\mathbb{Z}_p[G], \mathrm{sd}) \otimes_\mathbb{Z} \mathbb{Q}$, $BR_0(G) = br_0(G) \otimes_\mathbb{Z} \mathbb{Q}$, $BR_p(G) = br_p(G) \otimes_\mathbb{Z} \mathbb{Q}$. Regulator constants are multiplicative in direct sums of lattices and also under summing Brauer relations. As such, if $v_p(-)$ denotes the p-adic valuation, then there is a pairing

$$v_p(C_{(-)}(-))\colon BR_0(G) \times A(\mathbb{Z}_p[G], \mathrm{sd}) \longrightarrow \mathbb{Q}$$
$$(\theta, M) \longmapsto v_p(C_\theta(M)).$$

The space $BR_0(G)$ is always finite dimensional, whilst $A(\mathbb{Z}_p[G], \mathrm{sd})$ will regularly be infinite dimensional. For trivial reasons, elements of $BR_p(G)$ always lie in the kernel of $v_p(C_{(-)}(-))$. But, one might say that regulator constants are good invariants if the left kernel consists only of characteristic p relations. It is one of our main results that if G has cyclic Sylow p-subgroups, then this is always the case. But let us be more precise.

Outside of small families of groups we do not have classifications of the $\mathbb{Z}_p[G]$-lattices. On the other hand, the isomorphism classes of permutation modules, that is $\mathbb{Z}_p[G]$-lattices on which G acts by permuting a choice of basis, are easy to enumerate and it is possible to give a formula for their regulator constants in terms of group theoretic information. For this reason we shall primarily restrict our attention from $A(\mathbb{Z}_p[G], \mathrm{sd})$ to $A(\mathbb{Z}_p[G], \mathrm{perm})$, the subspace generated by permutation modules.

Again, for trivial reasons $A(\mathbb{Z}_p[G], \mathrm{cyc})$, the subspace generated by the permutation modules

$\mathbb{Z}_p[G/H]$ for $H \leq G$ cyclic, lies in the kernel of $v_p(C_{(-)}(-))$. We refer to the resulting pairing

$$\langle \ , \ \rangle_{\mathrm{perm}} \colon BR_0(G)/BR_p(G) \times A(\mathbb{Z}_p[G], \mathrm{perm})/A(\mathbb{Z}_p[G], \mathrm{cyc}) \to \mathbb{Q}$$

as the *permutation pairing*. A not immediately obvious fact is that both $BR_0(G)/BR_p(G)$ and $A(\mathbb{Z}_p[G], \mathrm{perm})/A(\mathbb{Z}_p[G], \mathrm{cyc})$ are canonically isomorphic to the free $\mathbb{Q}$-vector space on the set of conjugacy classes of p-hypo-elementary subgroups. With respect to this identification, the pairing is symmetric. Prior to quotienting the spaces need not have the same dimension and there is no such identification (cf. Remark 3.7).

THEOREM 1.1 *For a finite group G and prime p such that G has cyclic Sylow p-subgroups, the permutation pairing is non-degenerate.*

A formal consequence of Theorem 1.1 is that the isomorphism class of a permutation module M over $\mathbb{Z}_p$ is determined by its regulator constants and the isomorphism class of $M \otimes \mathbb{Q}_p$.

To show the theorem, we first reduce to p-hypo-elementary subgroups. All p-hypo-elementary groups with cyclic Sylow p-subgroups are of the form $C_{p^k} \rtimes C_n$ with $(p, n) = 1$. In this case, we find we are able to completely explicate the matrix representing the pairing, and showing invertibility becomes a combinatorial problem (Lemma 4.7).

For general G, the permutation pairing may be degenerate. For example, when $p = 3$, the group $C_3 \times C_3 \times S_3$ has a Brauer relation θ_Σ whose regulator constant is trivial on all permutation modules (see Section 7.3). I do not know if there are other lattices for which $C_{\theta_\Sigma}(-)$ does not vanish.

We do however provide a partial result for arbitrary G. For any group G, there is a canonical Brauer relation with leading term $[G]$ called the *Artin relation*, which we denote by θ_G (see Definition 2.14). Let $\mathbb{1}_G$ denote the trivial $\mathbb{Z}_p[G]$-module.

THEOREM 1.2 *For any finite group G and prime p, we have $v_p(C_{\theta_G}(\mathbb{1}_G)) \neq 0$.*

The proof is group theoretic in nature and completely independent of that of Theorem 1.1.

The final aspect of the paper is an extended application of Theorem 1.1. Suppose now that G has a cyclic Sylow p-subgroup P, and write $P_i \leq P$ for the subgroup of order p^i. For a $\mathbb{Z}_p[G]$-lattice M, Yakovlev [Yak96, Thm. 2.1] showed that the diagram

$$H^1(P_r, M) \underset{\longleftarrow}{\overset{\longrightarrow}{\rightleftarrows}} H^1(P_{r-1}, M) \underset{\longleftarrow}{\overset{\longrightarrow}{\rightleftarrows}} \quad \ldots \quad \underset{\longleftarrow}{\overset{\longrightarrow}{\rightleftarrows}} H^1(P_0, M) \qquad (\star)$$

determines the isomorphism class of M up to summands which are *trivial source*, i.e. summands of permutation modules. Here, the horizontal maps are restriction and corestriction, and each cohomology group is considered as an $N_G(P_i)$-module (cf. Section 6.2). Thus, M would be completely determined if one could provide invariants which constrain the remaining trivial source summand. We refer to $(\star)$ as the *Yakovlev diagram* of M.

Our main result gives conditions for when Theorem 1.1 can be used to determine the remaining trivial source summand of M. Denote by $A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$ the subring of the representation ring $A(\mathbb{Z}_{(p)}[G])$ generated by trivial source lattices (see Definition 6.1). Note that extension of scalars defines an inclusion $A(\mathbb{Z}_{(p)}[G]) \hookrightarrow A(\mathbb{Z}_p[G])$ [Rei70, Thm. 5.6 *iii)*] and so an isomorphism of the subrings generated by permutation modules $A(\mathbb{Z}_{(p)}[G], \mathrm{perm}) = A(\mathbb{Z}_p[G], \mathrm{perm})$. The condition is then that $A(\mathbb{Z}_{(p)}[G], \mathrm{triv}) = A(\mathbb{Z}_p[G], \mathrm{perm})$.

THEOREM 1.3 *Let G be a finite group and p a prime such that G has cyclic Sylow p-subgroups and such that $A(\mathbb{Z}_p[G], \mathrm{perm}) = A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$. Given two rationally self-dual $\mathbb{Z}_p[G]$-lattices M, N, then $M \cong N$ if and only if all the following conditions hold:*

3

i) $M \otimes \mathbb{Q}_p \cong N \otimes \mathbb{Q}_p$,

ii) for an explicit finite list of characteristic zero Brauer relations, the corresponding regulator constants of M, N are equal,

iii) M, N have isomorphic Yakovlev diagrams.

This is stated precisely as Theorem 6.8. It is relatively straightforward to obtain extensions of this result to arbitrary lattices (cf. Remark 6.9). If the conditions of the theorem hold for all p-hypo-elementary subgroups of G, then they hold for G. We also provide some explicit criteria for the condition $A(\mathbb{Z}_p[G], \mathrm{perm}) = A(\mathbb{Z}_p[G], \mathrm{triv})$ to be satisfied. Groups that satisfy the conditions include dihedral groups, abelian groups with cyclic Sylow p-subgroups and groups of order coprime to $(p-1)$.

For some groups, such as dihedral groups D_{2p} for primes $p \leq 67$, the isomorphism class of a $\mathbb{Z}[G]$-lattice M is determined by its localisations at the primes dividing $|G|$. As a result, Theorem 1.3 may be applied at each prime to give data which determines the isomorphism class of M as a $\mathbb{Z}[G]$-lattice (cf. Remark 7.1).

It is possible to define regulator constants $C_\theta(M)$ of a $\mathbb{Z}[G]$-lattice M. Then $C_\theta(M)$ is the product of the p-part of $C_\theta(M \otimes \mathbb{Z}_p)$ for all p dividing $|G|$ (see Remark 2.29). As a result, confining ourselves to $\mathbb{Z}_p[G]$-lattices over $\mathbb{Z}[G]$-lattices is innocuous.

As part of the author's PhD thesis, we shall describe some applications of Theorem 1.3 within number theory. For example, in the case of unit groups of number fields, when p divides $|G|$ at most once, it is possible to reinterpret the three invariants of Theorem 1.3 in terms of classical invariants of number fields [Tor18, Ch. 3].

Outline: In Section 2, we set out notation and recall necessary background results on Brauer relations and regulator constants. In Section 3, we outline precise questions on pairings arising from regulator constants. We also show that these reduce to considering p-hypo-elementary groups and that whenever the permutation pairing is non-degenerate, then permutation modules are determined by regulator constants and extension of scalars. In Section 4, we prove Theorem 1.1, and in Section 5, we prove Theorem 1.2. In Section 6, we apply Theorem 1.1 to prove Theorem 1.3 on determining lattices up to isomorphism. There we also provide criteria for groups to satisfy the conditions of Theorem 1.3. Finally, in Section 7, we provide examples and non-examples illustrating our results.

After reading Sections 2 and 3, the following Sections 4 and 5 may be read completely separately from each other, as may Section 6, which only requires the statement of Theorem 1.1.

2 Preliminaries

2.1 Notation

Throughout, G shall denote a finite group, p a prime and $\mathcal{R}$ any ring, but we will be most concerned with $\mathcal{R} = \mathbb{F}_p, \mathbb{Z}_{(p)}, \mathbb{Z}_p, \mathbb{Q}$ or $\mathbb{Q}_p$.

NOTATION 2.1 We fix the following notation:

- Let $\mathbb{1}_G$ or $\mathbb{1}$ denote the trivial $\mathcal{R}[G]$-module. Where the choice of ring requires emphasis we write $\mathbb{1}_{\mathcal{R},G}$.

- Given a subgroup $H \leq G$ and an $\mathcal{R}[G]$-module M, we shall denote the restriction of M to H by $M{\downarrow}_H^G$ or $M{\downarrow}_H$. Similarly, given an $\mathcal{R}[H]$-module N, we write $N{\uparrow}_H^G$ or $N{\uparrow}^G$ for the induction of N to G.

- We say that an $\mathcal{R}[G]$-module is an $\mathcal{R}[G]$-*lattice* if it is free of finite rank as an $\mathcal{R}$-module. Let $a(\mathcal{R}[G])$ denote the *representation ring* of G. As an abelian group, $a(\mathcal{R}[G])$ consists of formal $\mathbb{Z}$-linear combinations of isomorphism classes of $\mathcal{R}[G]$-lattices, subject to relations of the form $[M] + [N] = [M \oplus N]$. Here we use $[M]$, or just M, to denote the element of $a(\mathcal{R}[G])$ corresponding to an $\mathcal{R}[G]$-lattice M. The ring structure on $a(\mathcal{R}[G])$ is given by setting $[M] \cdot [N] = [M \otimes_{\mathcal{R}} N]$. Induction defines a group homomorphism $\mathrm{ind}\colon a(\mathcal{R}[H]) \to a(\mathcal{R}[G])$, whilst restriction defines a ring homomorphism $\mathrm{res}\colon a(\mathcal{R}[G]) \to a(\mathcal{R}[H])$.

- Let $A(\mathcal{R}[G])$ denote $a(\mathcal{R}[G]) \otimes \mathbb{Q}$. All our main results do not require the integral structure. As a result we frequently deal only with $A(\mathcal{R}[G])$ even though some intermediate results also hold integrally.

- Recall that a permutation module is a finite direct sum of modules of the form $\mathbb{1}{\uparrow}_H^G$ as H runs over subgroups of G. We denote the subgroup of $a(\mathcal{R}[G])$ spanned by such modules by $a(\mathcal{R}[G], \mathrm{perm})$. The equality $\mathbb{1}{\uparrow}_H^G \otimes_{\mathcal{R}} \mathbb{1}{\uparrow}_K^G = \mathbb{1}_H{\uparrow}^G{\downarrow}_K{\uparrow}^G$ and Mackey's formula show that $a(\mathcal{R}[G], \mathrm{perm}) \subseteq a(\mathcal{R}[G])$ is a subring, which we call the *permutation ring*. Both $\mathrm{res}, \mathrm{ind}$ restrict to maps of permutation rings, the former due to Mackey's formula. We set $A(\mathcal{R}[G], \mathrm{perm}) = a(\mathcal{R}[G], \mathrm{perm}) \otimes \mathbb{Q}$.

- Let $A(\mathcal{R}[G], \mathrm{cyc})$ be the $\mathbb{Q}$-subalgebra spanned by $\mathbb{1}{\uparrow}_H^G$ as H runs only over cyclic subgroups.

- Given a quotient $q\colon G \to G/N$ and an $\mathcal{R}[G/N]$-module M, we denote by $\mathrm{inf}_{G/N}^G(M)$ the inflation of M to G. This defines a ring homomorphism $\mathrm{inf}\colon a(\mathcal{R}[G/N]) \to a(\mathcal{R}[G])$, which restricts to a map of permutation rings since, for $H \leq G/N$, $\mathrm{inf}_{G/N}^G(\mathbb{1}_H{\uparrow}^{G/N}) = \mathbb{1}{\uparrow}_{q^{-1}(H)}^G$.

- In the same notation, given a G-module M, we define its deflation to G/N, $\mathrm{defl}_{G/N}^G M$, to be the fixed submodule M^N with G/N-action. Restricting to permutation modules, $(\mathbb{1}{\uparrow}_H^G)^N \cong \mathbb{1}{\uparrow}_{NH}^G$, so that $\mathrm{defl}(\mathbb{1}{\uparrow}_H^G) \cong \mathbb{1}{\uparrow}_{q(H)}^{G/N}$. The composite $\mathrm{defl}\circ\mathrm{inf}$ is the identity on all of $a(\mathcal{R}[G/N])$.

- By $H \leq_G G$, we denote a conjugacy class of subgroups of G with representative H. When used in indices, the symbol $\leq_G$ denotes indexing over conjugacy classes of subgroups. Thus, $\sum_{H \leq_G G} 1$ is equal to the number of conjugacy classes of subgroups.

REMARK 2.2 Recall that a module is called *indecomposable* if it can not be written as a direct sum of proper submodules. When $\mathcal{R} = \mathbb{Z}_p$ or $\mathbb{Q}$, every $\mathcal{R}[G]$-lattice admits a unique decomposition into direct sums of indecomposables [Rei70, Thm. 5.2], so that $a(\mathcal{R}[G])$ is free as a $\mathbb{Z}$-module with a basis given by isomorphism classes of indecomposable modules, but it need not have finite rank if $\mathcal{R} = \mathbb{Z}_p$ and p divides $|G|$ (see [CR94, Sec. 33]). Unique decomposition also ensures that for any two $\mathbb{Z}_p[G]$-lattices M, M', $[M] = [M'] \iff M \cong M'$.

If $\mathcal{R} = \mathbb{Z}_{(p)}$, then extension of scalars defines an inclusion $a(\mathbb{Z}_{(p)}[G]) \hookrightarrow a(\mathbb{Z}_p[G])$ [Rei70, Thm. 5.6 *iii)*] so we may again detect a lattice's isomorphism class from its class in the representation ring. However, $\mathbb{Z}_{(p)}[G]$-lattices need not admit unique decomposition into indecomposables [Ben06] and in general there is no obvious basis of $a(\mathbb{Z}_{(p)}[G])$. For simplicity, we shall often write $a(\mathbb{Z}_{(p)}[G]) \subseteq a(\mathbb{Z}_p[G])$.

2.2 Brauer relations

DEFINITION 2.3 A G-set is a set with a left action of G. We define the *Burnside ring* $b(G)$ of G to be the free abelian group on isomorphism classes of finite G-sets, quotiented by relations of the form $[X \coprod Y] - [X] - [Y]$ where X, Y are any G-sets, and $[X], [Y]$ are the corresponding elements of the free group. The ring structure is then given by setting $[X] \cdot [Y] = [X \times Y]$.

By decomposing G-sets into their orbits, we find that $b(G)$ is a free $\mathbb{Z}$-module on isomorphism classes of transitive G-sets. Every transitive G-set is of the form G/H for some subgroup $H \leq G$, where H is unique up to conjugacy. We denote the element of $b(G)$ corresponding to G/H by $[H]$. Thus, $b(G)$ is free as a $\mathbb{Z}$-module on the set of symbols $[H]$ for $H \leq_G G$.

We write $B(G)$ for $b(G) \otimes \mathbb{Q}$.

CONSTRUCTION 2.4 For any ring $\mathcal{R}$, a G-set X canonically defines a permutation module and we obtain a surjective map

$$b_{\mathcal{R}} \colon b(G) \to a(\mathcal{R}[G], \mathrm{perm}),$$

which sends $[H]$ to $\mathbb{1}_{\mathcal{R}, H} \uparrow^G$.

DEFINITION 2.5 A *Brauer relation*, of a group G over a ring $\mathcal{R}$, is an element of $\ker b_{\mathcal{R}} \subseteq b(G)$. We shall refer to the ideal $\ker b_{\mathcal{R}}$ as the space of Brauer relations over $\mathcal{R}$ and shall denote it by $br_{\mathcal{R}}(G)$.

When $\mathcal{R} = \mathbb{Q}$ or $\mathbb{F}_p$, we call a Brauer relation over $\mathcal{R}$ a relation in characteristic zero or characteristic p, respectively, and denote $br_{\mathcal{R}}(G)$ by $br_0(G), br_p(G)$ respectively. In the literature it is common to refer to a characteristic zero relation as simply a Brauer relation, and we shall often do the same.

EXAMPLE 2.6 If $G = S_3$, a characteristic zero Brauer relation is given by

$$\theta \colon [1] + 2[G] - [C_3] - 2[C_2].$$

We shall see that in fact, $br_0(S_3) = \theta \cdot \mathbb{Z}$.

All characteristic p relations are relations in characteristic zero also:

LEMMA 2.7 *As subspaces of $b(G)$, $br_p(G) = br_{\mathbb{Z}_{(p)}}(G) = br_{\mathbb{Z}_p}(G) \subseteq br_0(G)$.*

Proof. Via the factorisation $\mathbb{Z}_{(p)} \to \mathbb{Z}_p \to \mathbb{F}_p$, the map $b_{\mathbb{F}_p}$ factors as

$$b(G) \to a(\mathbb{Z}_{(p)}[G], \mathrm{perm}) \overset{M \mapsto M \otimes \mathbb{Z}_p}{\to} a(\mathbb{Z}_p[G], \mathrm{perm}) \overset{M \mapsto M \otimes \mathbb{F}_p}{\to} a(\mathbb{F}_p[G], \mathrm{perm}).$$

The middle map is an isomorphism by [Rei70, Thm 5.6 iii)], as is the last map by [Ben98, 3.11.4 i)], so the kernels of $b_{\mathbb{F}_p}, b_{\mathbb{Z}_{(p)}}$ and $b_{\mathbb{Z}_p}$ agree. As $b_{\mathbb{Q}}$ factors through $b_{\mathbb{Z}_{(p)}}$, there is an inclusion $br_{\mathbb{Z}_{(p)}}(G) \subseteq br_{\mathbb{Q}}(G)$. □

NOTATION 2.8 Let G be a finite group and $H \leq G$ a subgroup.

- Given an H-set X, we let $X\uparrow_H^G$ denote the induced G-set $(G \times X)/H$; here the H-equivalence is by acting on G on the right and X on the left, whilst G acts on the resulting set via its left action on G. For transitive G-sets (G/K) we have $(H/K)\uparrow^G = (G/K)$ and we shall regularly abuse notation by writing $[K]\uparrow^G$ simply as $[K]$, where now K is thought of as a subgroup of G.

- If Y is a G-set, we let $Y\downarrow_H^G$ denote its restriction to H. For a subgroup K of G, making good use of the above abuse of notation, Mackey's formula for G-sets states that

$$[K]\downarrow_H^G = \sum_{g \in K\backslash G/H} [K^g \cap H]. \tag{1}$$

If now $N \trianglelefteq G$ is a normal subgroup with quotient $q \colon G \to G/N$, then

- given a G/N-set X, we denote by $\inf_{G/N}^G X$ the inflated set X, on which elements of G act via their image in the quotient. For $H \leq G/N$, $\inf_{G/N}^G([H]) = [q^{-1}(H)]$,

- given a G-set Y, let $\mathrm{defl}_{G/N}^G Y$ denote its deflation, i.e. the set Y^N with its action of G/N. For a transitive G-set G/H, the fixed points under N is isomorphic to G/NH, which as a G/N-set is $(G/N)/q(H)$. In other words, $\mathrm{defl}_{G/N}^G([H]) = [q(H)]$, and thus $\mathrm{defl} \circ \inf$ is the identity map.

All of these operations induce group homomorphisms on Burnside rings, but only restriction and inflation will in general be ring homomorphisms. Each of $\mathrm{ind}, \mathrm{res}, \inf, \mathrm{defl}$ commute with $b_{\mathcal{R}}$. As a result, each restricts to morphisms of $br_{\mathcal{R}}(-)$.

2.3 Relations in characteristic zero

Finding an explicit basis, for an arbitrary finite group G, of the $br_0(G)$ is a hard problem, which was recently completed by Bartel-Dokchitser [BD15, BD14]. On the other hand, in this section we recall that, a basis of the space $br_0(G) \otimes \mathbb{Q}$ is provided by Artin's induction theorem.

NOTATION 2.9 Let $\mathrm{cyc}(G) := \{H \leq_G G \mid H\text{–cyclic}\}$ denote a set of representatives of each conjugacy class of cyclic subgroups.

THEOREM 2.10 (Artin's induction theorem [Sna94, Thm. 2.1.3]) *For any finite group G and $\mathbb{Q}[G]$-module M, there exists a unique $\alpha_H \in \mathbb{Q}$ for each cyclic $H \leq_G G$ such that*

$$M = \sum_{H \in \mathrm{cyc}(G)} \alpha_H \mathbb{1}_H \uparrow^G \in A(\mathbb{Q}[G]).$$

DEFINITION 2.11 We say that an element $\theta \in B(G)$ is supported at some set S of conjugacy classes of subgroups of G if the only $[H]$ with non-zero coefficients lie in S.

COROLLARY 2.12 *For any finite group G,*

  i) *the rank of $br_0(G)$ is equal to the number of conjugacy classes of non-cyclic subgroups of G,*

 ii) *there are no non-zero characteristic zero Brauer relations supported only at cyclic subgroups.*

Proof. Immediate. $\qquad\square$

Note that a group G is cyclic if and only if it has no non-trivial Brauer relations.

DEFINITION 2.13 For any ring $\mathcal{R}$ and finite group G, let $b_{\mathcal{R},\mathbb{Q}}$ denote the base change of $b_{\mathcal{R}}$,

$$b_{\mathcal{R},\mathbb{Q}} \colon B(G) \to A(\mathcal{R}[G], \mathrm{perm}).$$

We shall also call an element of the kernel of $b_{\mathcal{R},\mathbb{Q}}$ a Brauer relation over $\mathcal{R}$ and refer to the kernel $BR_{\mathcal{R}}(G) := br_{\mathcal{R}}(G) \otimes \mathbb{Q}$ as the space of Brauer relations over $\mathcal{R}$. Where there is ambiguity, we shall refer to elements of the kernel of $b_{\mathcal{R}}$ as *integral Brauer relations* and of $b_{\mathcal{R},\mathbb{Q}}$ as *rational Brauer relations*.

Induction theorems of the form of Theorem 2.10 always give rise to a corresponding family of (possibly rational) Brauer relations.

DEFINITION 2.14 For any group G, let

$$\mathbb{1}_G = \sum_{H \in \mathrm{cyc}(G)} \alpha_H \mathbb{1}_H {\uparrow}^G,$$

where the $\alpha_H \in \mathbb{Q}$ are given uniquely by Artin's induction theorem. Then,

$$\theta_G = [G] - \sum_{H \in \mathrm{cyc}(G)} \alpha_H [H] \in B(G)$$

is a rational Brauer relation of G. We call θ_G the *Artin relation* of G. Note that if G is cyclic, then $\theta_G = 0 \in B(G)$, otherwise θ_G is non-zero and has $[G]$-coefficient 1. The uniqueness statement of Artin's induction theorem shows that θ_G is, up to scaling, the unique element of $BR_0(G)$ supported only at G and cyclic subgroups.

The following example will be returned to in Section 4.2.

EXAMPLE 2.15 Let G be of the form $C_{p^r} \rtimes C_n$, with $p \nmid n$, and denote by $S \leq C_n$ the kernel of the action $C_n \to \mathrm{Aut}(C_{p^r})$. Writing s for $|S|$, we claim that

$$\theta_G = \frac{s}{n} \cdot [S] - [C_n] - \frac{s}{n} \cdot [C_{p^r} \times S] + [C_{p^r} \rtimes C_n],$$

which can be checked by direct calculation. If the action of C_n is not faithful, then S is a non-trivial subgroup of G and quotienting by S results in a group of the same form but with faithful action. The Artin relation of G is then the inflation of the Artin relation of G/S (using that the preimage of a cyclic subgroup of G/S is a cyclic subgroup of G).

Following Notation 2.8, when it is contextually clear we are referring to G-relations, for a subgroup $H \leq G$, we shall denote the G relation $\theta_H {\uparrow}^G$ simply by θ_H. Artin relations are well behaved under restriction:

LEMMA 2.16 *Let G be a finite group and H, K subgroups. Then,*

i) the restriction of the Artin relation of G to H is the Artin relation of H, i.e.

$$\theta_G {\downarrow}_H = \theta_H,$$

ii) more generally

$$\theta_H {\uparrow}_H^G {\downarrow}_K = \sum_{g \in H \backslash G / K} \theta_{H^g \cap K} {\uparrow}^K. \tag{2}$$

Proof. We prove *ii)*. Mackey's formula (1) states that

$$[H]\!\downarrow_K = \sum_{g \in H \backslash G / K} [H^g \cap K].$$

Also by Mackey, for any cyclic group $L \leq H$, $[L]\!\uparrow_H^G\!\downarrow_K$ is supported at cyclic subgroups. But then $\theta\!\uparrow_H^G\!\downarrow_K$ and $\sum_{g \in H \backslash G / K} \theta_{H^g \cap K}\!\uparrow^K$ are two relations whose coefficients agree at all non-cyclic subgroups and since there are no relations supported at cyclic subgroups (Corollary 2.12 *ii)*), they must therefore be equal. ◻

LEMMA 2.17 *A basis of the space of rational Brauer relations $BR_0(G)_{\mathbb{Q}}$ is given by the set $\{\theta_H\}$ of Artin relations for non-cyclic $H \leq_G G$.*

Proof. The θ_H are linearly independent as each is zero on non-cyclic subgroups other than $[H]$ and must span by Corollary 2.12 *i)*. ◻

2.4 Relations in characteristic p

DEFINITION 2.18 Let p be prime. A finite group G is called *p-hypo-elementary*, or simply p-hypo, if G has a normal Sylow p-subgroup P and G/P is cyclic, i.e. if G can be written in the form $P \rtimes C_n$ for P a p-group and $(p, n) = 1$.

NOTATION 2.19 We denote a set $\{H \leq_G G \mid H$ p-hypo$\}$ of representatives of the conjugacy classes of p-hypo-elementary subgroups by $\mathrm{hyp}_p(G)$. Similarly, let $\mathrm{nchyp}_p(G) := \{H \leq_G G \mid H$ is p-hypo and non-cyclic$\}$.

Recall that characteristic p relations are coincide with $\mathbb{Z}_{(p)}$ and $\mathbb{Z}_p$-relations (Lemma 2.7). Analogously to Corollary 2.12 we have

THEOREM 2.20 *For any finite group G,*

  i) a basis of $A(\mathbb{Z}_p[G], \mathrm{perm})$ is given by $\{\mathbb{1}\!\uparrow_H^G\}_{H \in \mathrm{hyp}_p(G)}$,

 ii) the rank of $\mathrm{br}_p(G)$ is equal to the number of conjugacy classes of non-p-hypo-elementary subgroups of G,

iii) there are no non-zero characteristic p Brauer relations supported only at p-hypo-elementary subgroups.

Proof. The first statement is a consequence of Conlon's induction theorem as we show later in Theorem 6.20. Given *i)*, both *ii)* and *iii)* are automatic. ◻

The first part also holds with $\mathbb{Z}_p$ replaced by $\mathbb{F}_p$ or $\mathbb{Z}_{(p)}$.

Note that there are no non-zero characteristic p Brauer relations for p-hypo-elementary groups, and this is only true of such groups. As before, the theorem gives rise to privileged relations in characteristic p:

DEFINITION 2.21 For any group G and prime p, write $\mathbb{1}_{\mathbb{Z}_p, G} = \sum_{H \in \mathrm{hyp}_p(G)} \alpha_H \mathbb{1}_{\mathbb{Z}_p, H}\!\uparrow_H^G$ with $\alpha_H \in \mathbb{Q}$ uniquely by Theorem 2.20. Since $BR_{\mathbb{Z}_p}(G) = BR_p(G)$ (Lemma 2.7),

$$\theta_{\mathrm{Con}, G} = [G] - \sum_{H \in \mathrm{hyp}_p(G)} \alpha_H [H]$$

9

is a rational Brauer relation in characteristic p, which we refer to as the *Conlon relation* of G. Note, $\theta_{\mathrm{Con},G}$ is identically zero if and only if G is p-hypo-elementary. The Conlon relation is the unique p-relation supported only at G and p-hypo-elementary subgroups. However, the Conlon relation need not be unique amongst characteristic zero relations supported at these groups.

As before, when it is clear that we are referring to G-relations, for a subgroup $H \leq G$, we denote $\theta_{\mathrm{Con},H}{\uparrow}^G$ simply by $\theta_{\mathrm{Con},H}$. All characteristic p relations are rational linear combinations of Conlon relations:

LEMMA 2.22 *Let G be a finite group and p a prime. Then,*

  i) *a basis of $BR_p(G)$ is formed by the set $\{\theta_{Con,H}\}$ as H runs over conjugacy classes of non-p-hypo-elementary groups,*

  ii) *this can be extended to a basis of $BR_0(G)$ by adding the Artin relations θ_H as H runs over conjugacy classes of non-cyclic p-hypo-elementary groups.*

Proof. The proof of *i)* is as in Lemma 2.17. For *ii)*, in addition use Corollary 2.12, Theorem 2.20. $\qquad\square$

EXAMPLE 2.23 Let $G = D_{2p} = C_p \rtimes C_2$ be the dihedral group of order $2p$ for p an odd prime. If ℓ is any prime, then

$$\{H \leq_G G \mid H \text{ is } \ell\text{-hypo-elementary}\} = \begin{cases} \{1\}, C_2, C_p & \ell \neq p \\ \{1\}, C_2, C_p, D_{2p} & \ell = p \end{cases}, \tag{3}$$

and so $\dim_{\mathbb{Q}} A(\mathbb{Z}_\ell[G], \mathrm{perm})$ is 3 unless $\ell = p$ when it is 4. A basis S of $A(\mathbb{Z}_p[G], \mathrm{perm})$ is formed by

$$S = \begin{cases} \mathbb{1}_{\{1\}}{\uparrow}^G, \mathbb{1}_{C_2}{\uparrow}^G, \mathbb{1}_{C_p}{\uparrow}^G & \ell \neq p \\ \mathbb{1}_{\{1\}}{\uparrow}^G, \mathbb{1}_{C_2}{\uparrow}^G, \mathbb{1}_{C_p}{\uparrow}^G, \mathbb{1}_G & \ell = p \end{cases}.$$

Since G has up to conjugacy four subgroups, of which three are cyclic, $\mathrm{rk}\, BR_0(G) = 1$. Let $\theta \in br_0(G)$ be the relation

$$\theta \colon 2[G] - [C_p] - 2[C_2] + [1].$$

Then $\theta = 2\theta_G$. As θ is indivisible as an element of $b(G)$, we find $br_0(G) = \theta \cdot \mathbb{Z}$.

Since $\mathrm{rk}\, br_\ell(G)$ is the number of conjugacy classes of non-p-hypo-elementary subgroups, by (3), $\mathrm{rk}\, br_\ell(G)$ is also one unless $\ell = p$ when it is zero. Given that $br_\ell(G) \subseteq br_0(G)$ (Lemma 2.7), we find

$$br_\ell(G) = \begin{cases} \theta \cdot \mathbb{Z} & \text{if } \ell \neq p \\ 0 & \text{if } \ell = p \end{cases}.$$

The Conlon relation $\theta_{\mathrm{Con},G}$ is equal to the Artin relation unless $\ell = p$ when it is zero.

2.5 Regulator constants

In this section, we recall how to associate to a characteristic zero Brauer relation, a function on (nice) $\mathcal{R}[G]$-lattices called its regulator constant.

We follow the construction given in [DD09] for an arbitrary PID $\mathcal{R}$ of characteristic zero. We are only ever concerned with $\mathcal{R} = \mathbb{Z}, \mathbb{Z}_{(p)}$ or $\mathbb{Z}_p$. Let $\mathcal{K}$ denote the field of fractions of $\mathcal{R}$.

DEFINITION 2.24 An $\mathcal{R}[G]$-lattice M is called *rationally self-dual* if $M \otimes \mathcal{K}$ is self-dual, i.e. $M \otimes \mathcal{K}$ is isomorphic to its linear dual $\mathrm{Hom}_{\mathcal{K}}(M \otimes \mathcal{K}, \mathcal{K})$ as $\mathcal{K}[G]$-modules. This is equivalent to the existence of a non-degenerate G-invariant inner product on $M \otimes \mathcal{K}$. If an inner product on $M \otimes \mathcal{K}$ exists, there is a restricted G-invariant inner product on M.

Rational self-duality is preserved under induction, restriction, inflation and deflation, as well as taking tensor products of two rationally self-dual lattices. We say that an element of $A(\mathcal{R}[G])$ is *rationally self-dual* if it can be written as a linear combination of self-dual lattices. We denote the subring of self-dual lattices by $a(\mathcal{R}[G], \mathrm{sd})$ and define $A(\mathcal{R}[G], \mathrm{sd})$ accordingly.

A rationally self-dual lattice M need not be linearly self-dual, i.e. a rationally self-dual M need not be isomorphic to $\mathrm{Hom}(M, \mathcal{R})$. If $\mathcal{R} = \mathbb{Z}$ or $\mathbb{Z}_{(p)}$, then, as all $\mathbb{Q}[G]$-modules are self-dual, all $\mathcal{R}[G]$-lattices are rationally self-dual.

DEFINITION 2.25 Let G be a finite group and $\theta = \sum_i [H_i] - \sum_j [H_j'] \in br_0(G)$ be an integral characteristic zero Brauer relation of G. Given a rationally self-dual $\mathcal{R}[G]$-lattice M, fix a choice of non-degenerate G-invariant inner product $\langle \ , \ \rangle$ on M. The *regulator constant* of θ evaluated at M is then

$$C_\theta(M) = \frac{\prod_i \det\left(\frac{1}{|H_i|}\langle \ , \ \rangle|_{M^{H_i}}\right)}{\prod_j \det\left(\frac{1}{|H_j'|}\langle \ , \ \rangle|_{M^{H_j'}}\right)} \in \mathcal{K}^\times/(\mathcal{R}^\times)^2.$$

This is independent of the choice of $\langle \ , \ \rangle$ as an element of $\mathcal{K}^\times/(\mathcal{R}^\times)^2$ (see [DD09, Thm. 2.17]). For M a $\mathbb{Z}[G]$ or $\mathbb{Z}_{(p)}[G]$-lattice, we may take the pairing to be positive definite and so for all characteristic zero Brauer relations θ and modules M we have $C_\theta(M) > 0$.

REMARK 2.26 When evaluating regulator constants at the trivial module, the formula simplifies. For example, if $\theta = \sum_i [H_i] - \sum_j [H_j']$, then

$$C_\theta(\mathbb{1}_G) = \frac{\prod_i \frac{1}{|H_i|}}{\prod_j \frac{1}{|H_j'|}} = \frac{\prod_j |H_j'|}{\prod_i |H_i|}. \tag{4}$$

This formula can be extended to permutation modules due to the formalism of regulator constants provided by the next lemma. That regulator constants of permutation modules can be made explicit in this way is crucial in the proof of Theorem 4.1.

LEMMA 2.27 ([DD09]) *Let G be any finite group and H a subgroup and let $\mathcal{R}, \mathcal{K}$ be as above. Assume throughout that all modules are rationally self-dual. Then,*

    i) if M, N are two $\mathcal{R}[G]$-lattices, then for any Brauer relation θ of G, $C_\theta(M \oplus N) = C_\theta(M)C_\theta(N)$,

    ii) if θ, θ' are two Brauer relations for G and M any $\mathcal{R}[G]$-lattice, then $C_{(\theta+\theta')}(M) = C_\theta(M)C_{\theta'}(M)$,

    iii) if M is a $\mathcal{R}[G]$-lattice, then $C_{\theta\uparrow_H^G}(M) = C_\theta(M\downarrow_H^G)$,

    iv) if M is a $\mathcal{R}[H]$-lattice, then $C_\theta(M\uparrow_H^G) = C_{\theta\downarrow_H^G}(M)$,

    v) if H is normal, then given a relation of G/H and a $\mathcal{R}[G]$-lattice M, $C_{\inf_{G/H}^G \theta}(M) = C_\theta(\mathrm{defl}_{G/H}^G M)$,

    vi) for any inclusion $\mathcal{R} \hookrightarrow \mathcal{T}$, with $\mathcal{T}$ a PID, any relation θ, and $\mathcal{R}[G]$-lattice M, we have $C_\theta(M) = C_\theta(M \otimes \mathcal{T}) \in \mathcal{L}^\times/(\mathcal{T}^\times)^2$ where $\mathcal{L}$ denotes the field of fractions of $\mathcal{T}$.

NOTATION 2.28 By definition, regulator constants of rationally self-dual $\mathbb{Z}_p[G]$-modules take values

in $\mathbb{Q}_p^\times/(\mathbb{Z}_p^\times)^2$. Let $v_p \colon \mathbb{Q}_p^\times \to \mathbb{Z}$ denote the usual p-adic valuation. This descends to a function $v_p \colon \mathbb{Q}_p^\times/(\mathbb{Z}_p^\times)^2 \to \mathbb{Z}$. For any prime $\ell \neq p$, we also have a "valuation at ℓ" function $\mathbb{Q}_p^\times/(\mathbb{Z}_p^\times)^2 \to \mathbb{Z}/2\mathbb{Z}$, which we also denote by v_ℓ.

REMARK 2.29 Since the regulator constant of a $\mathbb{Z}[G]$-lattice is always a positive rational number (see Definition 2.25), Lemma 2.27 *vi)* shows that the regulator constant $C_\theta(M)$ of a $\mathbb{Z}[G]$-lattice M is a function of the values $v_p(C_\theta(M \otimes \mathbb{Z}_p))$ as p runs over all primes.

The following observation will be crucial:

LEMMA 2.30 ([Bar12, Lem. 3.6]) *If G is a finite group and θ a relation in characteristic ℓ, then for any prime p (possibly equal to ℓ) and M any $\mathbb{Z}[G]$ or rationally self-dual $\mathbb{Z}_p[G]$-lattice we have*

$$v_\ell(C_\theta(M)) = 0.$$

REMARK 2.31 If G is a finite group and p is a prime not dividing the order of G, then the p-hypo-elementary subgroups of G are the cyclic subgroups and so all characteristic zero relations are characteristic p relations (Lemma 2.22). Thus Lemma 2.30 shows that the only prime powers appearing in regulator constants divide the order of the group. If G itself is ℓ-hypo-elementary, then, for $p \neq \ell$, all its p-hypo-elementary subgroups are cyclic and so all its characteristic 0 relations are relations in characteristic p and its regulator constants are always ℓ^{th} powers.

3 Pairings from regulator constants

In this section, we remark that the construction of regulator constants canonically defines a pairing between Brauer relations and rationally self-dual $\mathbb{Z}_p[G]$-lattices. This pairing has obvious Brauer relations and lattices which must lie in the kernel, but it is unclear what the kernels should be in general. Sections 4 and 5 can be seen as partial results in this direction. Finally, we show that non-degeneracy of such pairings leads to methods to determine the isomorphism classes of permutation modules.

3.1 The regulator constant pairing

CONSTRUCTION 3.1 Let G be any finite group and p a prime. The map

$$
\begin{aligned}
v_p(C_{(-)}(-)) \colon br_0(G) \times a(\mathbb{Z}_p[G], \mathrm{sd}) &\longrightarrow \mathbb{Z} \\
(\theta, M) &\longmapsto v_p(C_\theta(M)),
\end{aligned}
$$

is bi-additive (Lemma 2.27 *i),ii)*). Extending $\mathbb{Q}$-linearly we get a pairing,

$$v_p(C_{(-)}(-)) \colon BR_0(G) \times A(\mathbb{Z}_p[G], \mathrm{sd}) \longrightarrow \mathbb{Q},$$

which we also denote by $v_p(C_{(-)}(-))$ and which we call the *regulator constant pairing*. By Lemma 2.30, this factors as

$$v_p(C_{(-)}(-)) \colon BR_0(G)/BR_p(G) \times A(\mathbb{Z}_p[G], \mathrm{sd}) \longrightarrow \mathbb{Q}.$$

In Section 7.1, we calculate the full regulator constant pairing for dihedral groups D_{2p} with p odd, one of the few families of groups where a classification of all indecomposable lattices exists.

REMARK 3.2 The pairing $v_p(C_{(-)}(-))$ is far from non-degenerate; $A(\mathbb{Z}_p[G], \text{sd})$ is often infinite dimensional whilst $BR_0(G)$ is always finite dimensional. Explicit elements of the right kernel are given by taking a lattice $M\uparrow_H^G$ induced from a cyclic subgroup H. This pairs to zero with all relations since

$$v_p(C_\theta(M\uparrow_H^G)) = v_p(C_{\theta\downarrow_H^G}(M)) = 0,$$

where first equality is Lemma 2.27 *iv)* and the second is because cyclic groups have no non-zero Brauer relations (Corollary 2.12). The behaviour of the left kernel is less clear:

QUESTION 3.3 Are there groups for which the left kernel of $v_p(C_{(-)}(-))\colon BR_0(G)/BR_p(G) \times A(\mathbb{Z}_p[G], \text{sd}) \to \mathbb{Q}$ is non-trivial?

It is also interesting to replace $\mathbb{Z}_p$ with other rings. For $\mathbb{Z}_{(p)}$ and so also for $\mathbb{Z}_p$, if G has cyclic Sylow p subgroups, then the left kernel is trivial (see Theorem 4.1). Outside of this case, things are less clear and there are some very small groups (e.g. $C_3 \times C_3 \times S_3$ when $p = 3$) for which we have been unable to determine the left kernel. There are groups with Brauer relations which pair trivially with all summands of permutation modules but are not relations in characteristic p (namely for $C_3 \times C_3 \times S_3$, see Section 7.2). On the other hand, the kernel is never all of $BR_0(G)$ (Theorem 5.1).

LEMMA 3.4 *Let θ be a relation of a finite group G. For any prime p the following are equivalent,*

i) $v_p(C_\theta(-))\colon A(\mathbb{Z}_p[G], \text{sd}) \to \mathbb{Q}$ *vanishes identically,*

ii) $v_p(C_{\theta\downarrow_H}(-))\colon A(\mathbb{Z}_p[H], \text{sd}) \to \mathbb{Q}$ *vanishes identically for all conjugacy classes of p-hypo-elementary subgroups $H \leq G$.*

Proof. For the forward direction, use that $v_p(C_{\theta\downarrow_H}(M)) = v_p(C_\theta(M\uparrow^G)) = 0$ (Lemma 2.27 *iv)*). For the reverse, write $\mathbb{1} = \sum_{H\in\text{hyp}_p(G)} \alpha_H \mathbb{1}_H\uparrow^G$ as in the Conlon relation. Then for any rationally self-dual $\mathbb{Z}_p[G]$-lattice

$$M = M \otimes \mathbb{1} = \sum_{H\in\text{hyp}_p(G)} \alpha_H \cdot (M \otimes \mathbb{1}\uparrow_H^G) = \sum_{H\in\text{hyp}_p(G)} \alpha_H \cdot M\downarrow_H\uparrow_H^G,$$

where the $M\downarrow_H$ are rationally self-dual. Then,

$$v_p(C_\theta(M)) = \sum_{H\in\text{hyp}_p(G)} \alpha_H v_p(C_\theta(M\downarrow_H\uparrow_H^G)) = \sum_{H\in\text{hyp}_p(G)} \alpha_H v_p(C_{\theta\downarrow_H}(M\downarrow_H)) = 0$$

. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

LEMMA 3.5 *For any finite group G, the following are equivalent:*

i) *the left kernel of $v_p(C_{(-)}(-))\colon BR_0(G)/BR_p(G) \times A(\mathbb{Z}_p[G], \text{sd}) \to \mathbb{Q}$ is trivial,*

ii) *the left kernel of $v_p(C_{(-)}(-))\colon BR_0(G/N)/BR_p(G/N) \times A(\mathbb{Z}_p[G/N], \text{sd}) \to \mathbb{Q}$ is trivial for all normal subgroups N.*

Moreover, both are implied by

iii) *the left kernels of $v_p(C_{(-)}(-))\colon BR_0(H) \times A(\mathbb{Z}_p[H], \text{sd}) \to \mathbb{Q}$ are trivial for all isomorphism classes of p-hypo-elementary subgroups $H \leq G$.*

Proof. To see *i)* $\implies$ *ii)*, suppose that the left kernel of the pairing for G is trivial and let θ be a relation for G/N which is not a relation in characteristic p. Since $\text{defl} \circ \text{inf} = \text{id}$ and both take characteristic p relations to characteristic p relations, $\text{inf}\,\theta$ must also not be a p-relation. So, by

assumption, there exists an M for which $0 \neq v_p(C_{\inf\theta}(M))$. By Lemma 2.27 *v)*, $v_p(C_{\inf\theta}(M)) = v_p(C_\theta(\mathrm{defl}M)) \neq 0$ and $v_p(C_\theta(-))$ doesn't vanish identically. The reverse direction is automatic.

Now assume *iii)*. By Lemma 3.4, $v_p(C_\theta(-))$ vanishes if and only if $v_p(C_{\theta\downarrow_H}(-))$ vanishes for all H. But if θ is not a relation in characteristic p, there exists a p-hypo-elementary subgroup H for which $\theta\downarrow_H \neq 0$ (use Lemma 2.22 *i)*) and so $v_p(C_{\theta\downarrow_H}(-))$ doesn't vanish. $\qquad\square$

3.2 The permutation pairing

In this section, we study the restriction of the regulator constant pairing to permutation modules. Here we have a chance to be much more explicit as Theorem 2.20 describes a basis of $A(\mathbb{Z}_p[G], \mathrm{perm})$, and regulator constants of permutation modules are easy to calculate.

NOTATION 3.6 Let $P(G)$ denote the free $\mathbb{Q}$-vector space on the set of conjugacy classes of non-cyclic p-hypo-elementary subgroups.

REMARK 3.7 As in Remark 3.2, if we restrict to $A(\mathbb{Z}_p[G], \mathrm{perm})$, then $v_p(C_{(-)}(-))$ factors as

$$v_p(C_{(-)}(-))\colon BR_0(G)/BR_p(G) \times A(\mathbb{Z}_p[G], \mathrm{perm})/A(\mathbb{Z}_p[G], \mathrm{cyc}) \to \mathbb{Q}.$$

Lemma 2.22 *ii)* demonstrates that $P(G)$ is canonically isomorphic to $BR_0(G)/BR_p(G)$ (via $H \mapsto \theta_H$). On the other hand, Theorem 2.10 shows that $P(G)$ is canonically identified with $A(\mathbb{Z}_p[G], \mathrm{perm})/A(\mathbb{Z}_p[G], \mathrm{cyc})$ by sending H to $\mathbb{1}\uparrow_H^G$.

It is not true that the spaces can be identified before factoring v_p. Indeed, $BR_0(G)$ is of dimension equal to the number of non-cyclic subgroups, whereas $A(\mathbb{Z}_p[G], \mathrm{perm})$ is of dimension equal to the number of non-p-hypo-elementary subgroups.

CONSTRUCTION 3.8 Via these canonical identifications, we may consider the restricted pairing of Remark 3.7 as a pairing

$$\langle\ ,\ \rangle_{\mathrm{perm}}\colon P(G) \times P(G) \longrightarrow \mathbb{Q},$$

sending (H, K) to $v_p(C_{\theta_H}(\mathbb{1}\uparrow_K^G))$. We call $\langle\ ,\ \rangle_{\mathrm{perm}}$ the *permutation pairing*.

LEMMA 3.9 *For any finite group G and prime p, $\langle\ ,\ \rangle_{\mathrm{perm}}\colon P(G) \times P(G) \longrightarrow \mathbb{Q}$ is symmetric.*

Proof. For any two subgroups H and K of G, Lemmas 2.16, 2.27 show that

$$C_{\theta_H\uparrow^G}(\mathbb{1}_K\uparrow^G) = C_{\theta_H\uparrow^G\downarrow_K}(\mathbb{1}_K)$$
$$= \prod_{g\in H\backslash G/K} C_{\theta_{H^g\cap K}}(\mathbb{1}_{H^g\cap K}).$$

Whilst,

$$C_{\theta_K\uparrow^G}(\mathbb{1}_H\uparrow^G) = C_{\theta_K}(\mathbb{1}_H\uparrow^G\downarrow_K)$$
$$= C_{\theta_K}\left(\sum_{g\in H\backslash G/K} \mathbb{1}_{H^g\cap K}\uparrow^K\right)$$
$$= \prod_{g\in H\backslash G/K} \left(C_{\theta_{H^g\cap K}}(\mathbb{1}_{H^g\cap K})\right).$$

$\qquad\square$

REMARK 3.10 Along the same lines, Lemma 2.27 and (2) show that, for $H, K \leq G$,

$$
\begin{aligned}
\langle H, K \rangle_{\mathrm{perm}} &:= v_p(C_{\theta_H \uparrow^G}(\mathbb{1}_K \uparrow^G)) \\
&= v_p(C_{\theta_H \uparrow^G \downarrow_K}(\mathbb{1}_K)) \\
&= \sum_{g \in H \backslash G / K} C_{\theta_{H^g} \downarrow_{H^g \cap K} \uparrow^K}(\mathbb{1}_K) \\
&= \sum_{g \in H \backslash G / K} C_{\theta_{H^g \cap K} \uparrow^K}(\mathbb{1}_K) \\
&= \sum_{g \in H \backslash G / K} v_p(C_{\theta_{H^g \cap K}}(\mathbb{1}_{H^g \cap K})).
\end{aligned}
\tag{5}
$$

Combining this with (4) of p11 gives a formula for the permutation pairing.

It is tempting to ask if permutation pairing is non-degenerate for all groups G. This proves too naive, in Section 7.2, we exhibit a family of groups for which the permutation pairing is degenerate (e.g. $C_3 \times C_3 \times S_3$ when $p = 3$). Analogously to Lemmas 3.4, 3.5 we have:

LEMMA 3.11 *Let θ be a relation of a finite group G. For any prime p the following are equivalent,*

  i) $v_p(C_\theta(-))\colon A(\mathbb{Z}_p[G], \mathrm{perm}) \to \mathbb{Q}$ *vanishes identically,*

  ii) $v_p(C_{\theta \downarrow_H}(-))\colon A(\mathbb{Z}_p[H], \mathrm{perm}) \to \mathbb{Q}$ *vanishes identically for all conjugacy classes of p-hypo-elementary subgroups $H \leq G$.*

LEMMA 3.12 *For any finite group G, the following are equivalent:*

  i) *the permutation pairing is non-degenerate,*

  ii) *the permutation pairing of G/N is non-degenerate for all $N \trianglelefteq G$.*

  Moreover, both are implied by

  iii) *the permutation pairing of H is non-degenerate for all p-hypo-elementary subgroups H.*

The proofs are identical to before. As a result, we see that infinitely many groups exist where the permutation pairing is degenerate, for example, when $p = 3$, all groups with a $C_3 \times C_3 \times S_3$ quotient. We prove two main results on the permutation pairing. Theorem 4.1 states that the permutation pairing is non-degenerate for all groups with cyclic Sylow p-subgroups. Whilst, for arbitrary G, Theorem 5.1 states that the permutation pairing is not the zero pairing (unless $P(G) = 0$).

This leaves many open questions. For example:

QUESTION 3.13 Can one describe the groups for which the permutation pairing is degenerate?

It would also be interesting to know of the existence of a group with degenerate permutation pairing but for which the regulator constant pairing has trivial left kernel. There are also many hard problems which arise from considering these pairings integrally.

3.3 Regulator constants as invariants of permutation modules

The non-degeneracy of the permutation pairing is a measure of the strength of regulator constants as invariants of permutation modules. In this section, we show that the isomorphism class of an arbitrary $\mathbb{Z}_p[G]$-permutation module is determined by the isomorphism class of its extension

of scalars to $\mathbb{Q}_p$ and regulator constants if and only if the permutation pairing is non-degenerate.

CONSTRUCTION 3.14 Let $P''(G)$ denote the free $\mathbb{Q}$-vector space on conjugacy classes of cyclic subgroups. Artin's induction theorem (Thm. 2.10) states that there is a canonical isomorphism $P''(G) \xrightarrow{\sim} A(\mathbb{Q}[G])$ sending $H \to \mathbb{1}_{\mathbb{Q},H}\uparrow^G$. In the same way, $A(\mathbb{Z}_p[G], \text{cyc})$ is also canonically identified with $P''(G)$. Define a pairing

$$\langle \ , \ \rangle_{\text{char}} \colon P''(G) \times P''(G) \longrightarrow \mathbb{Q}$$
$$(H, K) \longmapsto \langle \mathbb{1}_{\mathbb{Z}_p, H}\uparrow^G \otimes \mathbb{Q}_p, \mathbb{1}_{\mathbb{Z}_p, K}\uparrow^G \otimes \mathbb{Q}_p \rangle_{\text{char}},$$

where the final inner product is the usual pairing given by character theory. Then, $\langle \ , \ \rangle_{\text{char}}$ is symmetric and is non-degenerate by Artin's induction theorem.

CONSTRUCTION 3.15 Let $P'(G)$ denote the free $\mathbb{Q}$-vector space on conjugacy classes of p-hypo-elementary subgroups of G. We define the pairing

$$\langle \ , \ \rangle_* \colon P'(G) \times P'(G) \longrightarrow \mathbb{Q}$$
$$(H, K) \longmapsto \begin{cases} \langle \mathbb{1}_{\mathbb{Z}_p, H}\uparrow^G \otimes \mathbb{Q}_p, \mathbb{1}_{\mathbb{Z}_p, K}\uparrow^G \otimes \mathbb{Q}_p \rangle_{\text{char}} & \text{if } H \text{ is cyclic} \\ v_p(C_{\theta_H}(\mathbb{1}_{\mathbb{Z}_p, K}\uparrow^G)) & \text{if } H \text{ is non-cyclic} \end{cases}.$$

This extends both $\langle \ , \ \rangle_{\text{perm}}$ and $\langle \ , \ \rangle_{\text{char}}$.

REMARK 3.16 The pairing $\langle \ , \ \rangle_*$ is chosen so that, via the identification $P'(G) \cong A(\mathbb{Z}_p[G], \text{perm})$, in the second variable, the construction extends to a pairing $P'(G) \times A(\mathbb{Z}_p[G]) \to \mathbb{Q}$ on the full representation ring (cf. Remark 6.17).

LEMMA 3.17 *For any finite group G, the following are equivalent,*

  i) *the permutation pairing of G is non-degenerate,*

 ii) *the pairing $\langle \ , \ \rangle_*$ is non-degenerate,*

iii) *the isomorphism class of an arbitrary permutation module over $\mathbb{Z}_p$ is determined by*

    a) *the isomorphism class of $M \otimes \mathbb{Q}_p$, and*

    b) *the valuations of the regulator constants $v_p(C_{\theta_H}(M))$ as H runs over elements of $\text{nchyp}_p(H)$.*

Proof. For equivalence of *i)* and *ii)*, note that, for any cyclic subgroup K, $v_p(C_{\theta_H}(\mathbb{1}\uparrow_K^G)) = 0$ (Remark 3.2). Thus, if we order the canonical basis of $P'(G)$ so that the cyclic subgroups come before the non-cyclic p-hypo-elementary subgroups, then the matrix representing $\langle \ , \ \rangle_*$ is block upper triangular, with diagonal blocks given by the matrices representing $\langle \ , \ \rangle_{\text{char}}$ and the permutation pairing respectively. The former is always invertible so $\langle \ , \ \rangle_*$ is non-degenerate if and only if the permutation pairing is.

The equivalence of *ii)* and *iii)* is automatic. $\qquad\square$

EXAMPLE 3.18 Let $G = D_{2p}$. Up to conjugacy, the p-hypo-elementary subgroups of G are $S = \{\{1\}, C_2, C_p, D_{2p}\}$. Applying (4) of p11 to θ_G as calculated in Example 2.15, we find $v_p(C_{\theta_G}(\mathbb{1}_G)) = -1/2$. Thus, the matrix representing $\langle \ , \ \rangle_*$ with respect to the basis of $P'(G)$ given by S is:

$$
\begin{array}{c c}
 & \begin{array}{cccc} \{1\} & C_2 & C_p & D_{2p} \end{array} \\
\begin{array}{c} \{1\} \\ C_2 \\ C_p \\ D_{2p} \end{array} &
\left(\begin{array}{ccc|c}
2p & p & 2 & 1 \\
p & (p+1)/2 & 1 & 1 \\
2 & 1 & 2 & 1 \\
\hline
0 & 0 & 0 & -1/2
\end{array} \right).
\end{array}
$$

In Section 7.1, we extend this to allow arbitrary $\mathbb{Z}_p[D_{2p}]$-lattices.

4 Non-degeneracy of the permutation pairing for groups with cyclic Sylow p-subgroups

In this section we prove:

THEOREM 4.1 *Let G be a finite group and p a prime such that G has cyclic Sylow p-subgroups. Then, the permutation pairing*

$$
v_p(C_{(-)}(-)) \colon BR_0(G)/BR_p(G) \times A(\mathbb{Z}_p[G], \mathrm{perm})/A(\mathbb{Z}_p[G], \mathrm{cyc}) \to \mathbb{Q}
$$

is non-degenerate.

As a result, for such groups G, the regulator constant pairing has trivial left kernel and we find:

COROLLARY 4.2 *Let G be a finite group and p a prime for which the Sylow p-subgroups of G are cyclic. Then, the isomorphism class of an arbitrary $\mathbb{Z}_p[G]$-permutation module M is determined by,*

  i) *the isomorphism class of $M \otimes \mathbb{Q}_p$,*

 ii) *the valuations of the regulator constants $v_p(C_{\theta_H}(M))$ as H runs over elements of $\mathrm{nchyp}_p(H)$.*

Proof. This follows by Lemma 3.17. □

The proof of Theorem 4.1 reduces to the case of G p-hypo-elementary. Since all p-hypo-elementary groups with cyclic Sylow p-subgroups are of the form $C_{p^k} \rtimes C_n$ with $(n, p) = 1$ we can then perform an explicit calculation.

4.1 GCD matrices

We first state and prove a purely combinatorial statement. Since this may be of limited independent interest this subsection is self contained.

NOTATION 4.3 For a natural number n and divisor s of n, denote by

  • $D'(n)$ the set of divisors of n (ordered increasingly),
  • $D(n, s) \subset D'(n)$ the set of divisors of n not dividing s,
  • $N(n)$ the symmetric matrix with rows and columns indexed by elements of $D'(n)$ and $(d_1, d_2)^{\mathrm{th}}$ entry given by $\gcd(d_1, d_2)$,
  • $M(n, s)$ the symmetric matrix with rows and columns indexed by elements of $D(n, s)$ and $(d_1, d_2)^{\mathrm{th}}$ entry given by $(\gcd(d_1, d_2) - \gcd(d_1, d_2, s))$.

EXAMPLE 4.4 If $n = 12$ and $s = 2$ then $D(12, 2) = \{3, 4, 6, 12\}$ and

$$
M(12,2) = \begin{array}{c} \\ 3 \\ 4 \\ 6 \\ 12 \end{array} \begin{array}{cccc} 3 & 4 & 6 & 12 \\ \begin{pmatrix} 2 & 0 & 2 & 2 \\ 0 & 2 & 0 & 2 \\ 2 & 0 & 4 & 4 \\ 2 & 2 & 4 & 10 \end{pmatrix} \end{array},
$$

which has full rank.

REMARK 4.5 Matrices of the form $N(n)$ are called GCD matrices and are always invertible (not necessarily integrally, see Lemma 4.6). Although matrices defined in a similar way to $M(n, s)$ have been studied (see [BL89, Beg10]), we have been unable to find results in the literature that directly cover matrices of the form $M(n, s)$. For this reason, we have included a full calculation of their determinants and thus invertibility. First we recall the proof of the determinant formula for $N(n)$.

LEMMA 4.6 *For any natural number n, the matrix $N(n)$ has determinant $\prod_{d \in D'(n)} \phi(d)$, where ϕ denotes Euler's totient function, and thus is always of full rank.*

Proof. For $n = p^e$ a prime power,

$$
N(p^e) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & p & \ldots & p \\ \vdots & \vdots & & \vdots \\ 1 & p & \ldots & p^e \end{pmatrix}.
$$

If $e > 1$, expanding the final column shows that $\det(N(p^e)) = (p^e - p^{e-1}) \det(N(p^{e-1})) = \phi(p^e) \det(N(p^{e-1}))$, as any $(e-1) \times (e-1)$ minor containing the first $(e-1)$ terms of the last two rows is not of full rank. Inductively this shows the determinant formula for prime powers.

Now let $s = rt$ with $(r, t) = 1$. Then, using the bijection $D'(rt) \leftrightarrow D'(r) \times D'(t)$, after simultaneous permutation of rows and columns (which preserves the determinant) $N(s)$ is of the form:

$$
N(s) = \begin{array}{c} \\ u_1 \\ u_2 \\ \vdots \\ u_k \end{array} \begin{array}{c} \begin{array}{cccc} u_1 & u_2 & \cdots & u_k \end{array} \\ \left(\begin{array}{c|c|c|c} \gcd(u_1, u_1)N(r) & \gcd(u_1, u_2)N(r) & \ldots & \gcd(u_1, u_k)N(r) \\ \hline \gcd(u_2, u_1)N(r) & \gcd(u_2, u_2)N(r) & \ldots & \gcd(u_2, u_k)N(r) \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline \gcd(u_k, u_1)N(r) & \gcd(u_k, u_2)N(r) & \ldots & \gcd(u_k, u_k)N(r) \end{array} \right) \end{array} = N(r) \otimes N(t),
$$

writing u_i for the elements of $D'(t)$. If A, B are matrices of dimension m, n respectively, then their tensor product satisfies the familiar formula

$$
\det(A \otimes B) = \det(A)^n \det(B)^m.
$$

Applying this inductively, using the bijection $D'(rt) \leftrightarrow D'(r) \times D'(t)$,

$$\det(N(r) \otimes N(t)) = \left(\prod_{d \in D'(r)} \phi(d) \right)^{|D'(t)|} \cdot \left(\prod_{l \in D'(t)} \phi(l) \right)^{|D'(r)|}$$

$$= \prod_{d \in D'(r)} \left(\phi(d)^{|D'(t)|} \prod_{l \in D'(t)} \phi(l) \right)$$

$$= \prod_{d \in D'(r)} \prod_{l \in D'(t)} \phi(d)\phi(l)$$

$$= \prod_{w \in D'(rt)} \phi(w),$$

as required. $\qquad \square$

LEMMA 4.7 *The matrix $M(n,s)$ has full rank for all natural numbers n and divisors s of n. Moreover, $\det(M(n,s)) = \prod_{d \in D(n,s)} \phi(d)$, where ϕ is the Euler totient function.*

Proof. We first prove the case when $s = 1$. Consider the matrix $N(n)$ (whose determinant equals $\prod_{d \in D'(n)} \phi(d)$ by Lemma 4.6). Within $N(n)$, the first row and column are constantly 1, and if we subtract the first column from all subsequent columns we get

$$\det(N(n)) = \det \begin{pmatrix} 1 & 0 & \dots & & 0 \\ 1 & & & & \\ \vdots & & M(n,1) & & \\ 1 & & & & \end{pmatrix} = \det(M(n,1)).$$

As $\phi(1) = 1$, this verifies the determinant formula in the case of $s = 1$.

We proceed by induction on the number of prime divisors of s. Assume that $M(n,s)$ has determinant

$$\det(M(n,s)) = \prod_{d \in D(n,s)} \phi(d),$$

and consider $M(p^r n, p^e s)$ with $p \nmid n, s$.

Let d be a divisor of $p^r n$, so d is of the form $p^k d'$ with $p \nmid d'$ and $0 \leq k \leq r$. Then, $d \in D(p^r n, p^e s) \iff$ either $k \leq e$ and $d' \in D(n,s)$, or $k > e$ and $d' \in D'(n)$. In other words, $D(p^r n, p^e s)$ can be partitioned as

$$D(p^r n, p^e s) = \left(\bigcup_{i=0}^{e} p^i D(n,s) \right) \cup \left(\bigcup_{i=e+1}^{r} p^i D'(n) \right).$$

Call $D_1 = \bigcup_{i=0}^{e} p^i D(n,s)$ and $D_2 = \bigcup_{i=p^{e+1}}^{r} p^i D'(n)$. Simultaneously reorder the rows and columns of $M(p^r n, p^e s)$ so that they respect this decomposition. Define A, B, C by

$$M(p^r n, p^e s) = \begin{array}{c} \\ D_1 \\ D_2 \end{array} \begin{array}{c} D_1 \quad D_2 \\ \left(\begin{array}{c|c} A & C \\ \hline C^T & B \end{array} \right) \end{array}.$$

For any two elements $p^{l_1} d_1, p^{l_2} d_2 \in D_1$, the corresponding entry of A is given by

$$\gcd(p^{l_1} d_1, p^{l_2} d_2) - \gcd(p^{l_1} d_1, p^{l_2} d_2, p^e s) = p^{\min\{l_1, l_2\}}(\gcd(d_1, d_2) - \gcd(d_1, d_2, s)).$$

So A is the tensor product

$$A = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & p & \ldots & p \\ \vdots & \vdots & & \vdots \\ 1 & p & \ldots & p^e \end{pmatrix} \otimes M(n, s) = N(p^e) \otimes M(n, s),$$

which has determinant

$$\det(A) = \det(N(p^e))^{|D(n,s)|} \cdot \det(M(n, s))^{e+1}.$$

By induction and Lemma 4.6,

$$
\begin{aligned}
\det(A) &= \det(N(p^e))^{|D(n,s)|} \cdot \det(M(n, s))^{e+1} \\
&= \left(\prod_{k=0}^{e} \phi(p^k)^{|D(n,s)|} \right) \cdot \left(\prod_{d \in D(n,s)} \phi(d)^{e+1} \right) \\
&= \prod_{k=0}^{e} \left(\phi(p^k)^{|D(n,s)|} \cdot \prod_{d \in D(n,s)} \phi(d) \right) \\
&= \prod_{k=0}^{e} \prod_{d \in D(n,s)} \phi(p^k)\phi(n) \\
&= \prod_{d \in D_1} \phi(d).
\end{aligned}
$$

We now row reduce to remove C^T. For $e < k \leq r$, let $v_{p^k d}$ denote the row vector with entries indexed by $D(n, s) = D_1 \cup D_2$ whose t^{th} entry is defined by

$$(v_{p^k d})_t = \gcd(p^e d, t) - \gcd(p^e d, t, p^e s).$$

If $d \mid s$, then $\gcd(p^e d, t) = \gcd(p^e d, t, p^e s)$ and $v_{p^k d}$ is identically zero. If $d \nmid s$, then $p^e d \in D_1$ and $v_{p^k d}$ is the $(p^e d)^{\text{th}}$ row of the matrix $M(n, s)$. In either case, subtracting $v_{p^k d}$ from the $(p^k d)^{\text{th}}$ row is an elementary row operation and preserves the rank and determinant.

Call $M'(p^r n, p^e s)$ the matrix resulting from performing this reduction for all elements of D_2. The entries of the $p^k d^{\text{th}}$ row for $p^k d \in D_2$ now satisfy, for $p^{k'} d' \in D_1$,

$$
\begin{aligned}
M'(p^r n, p^e s)_{p^k d, p^{k'} d'} &= \gcd(p^k d, p^{k'} d') - \gcd(p^k d, p^{k'} d', p^e s) - \gcd(p^e d, p^{k'} d') + \gcd(p^e d, p^{k'} d', p^e s) \\
&= p^{k'} \gcd(d, d') - p^{k'} \gcd(d, d', s) - p^{k'} \gcd(d, d') + p^{k'} \gcd(d, d', s) \\
&= 0,
\end{aligned}
$$

and for $p^{k'} d' \in D_2$,

$$
\begin{aligned}
M'(p^r n, p^e s)_{p^k d, p^{k'} d'} &= \gcd(p^k d, p^{k'} d') - \gcd(p^k d, p^{k'} d', p^e s) - \gcd(p^e d, p^{k'} d') + \gcd(p^e d, p^{k'} d', p^e s) \\
&= p^{\min\{k, k'\}} \gcd(d, d') - p^e \gcd(d, d', e) - p^e \gcd(d, d') + p^e \gcd(d, d', s) \\
&= (p^{\min\{k, k'\}} - p^e) \gcd(d, d').
\end{aligned}
$$

Therefore, the row reduction results in a matrix of the form

$$M'(p^r n, p^e s) = \begin{array}{c} \\ D_1 \\ D_2 \end{array} \begin{array}{c} D_1 \ \ D_2 \\ \left(\begin{array}{c|c} A & C \\ \hline 0 & B' \end{array} \right) \end{array} .$$

where

$$B' = N(n) \otimes \begin{pmatrix} p^{e+1} - p^e & p^{e+1} - p^e & \cdots & p^{e+1} - p^e \\ p^{e+1} - p^e & p^{e+2} - p^e & \cdots & p^{e+2} - p^e \\ \vdots & \vdots & & \vdots \\ p^{e+1} - p^e & p^{e+2} - p^e & \cdots & p^r - p^e \end{pmatrix}$$

$$= N(n) \otimes M(p^r, p^e)$$

$$= N(n) \otimes p^e M(p^{r-e}, 1).$$

Since

$$\det(M(p^r n, p^e s)) = \det(A) \cdot \det(B'),$$

to complete the proof we must show that $\det(B') = \prod_{d \in D_2} \phi(d)$. Indeed,

$$\det(B') = \det(N(n))^{r-e} \cdot \det(M(p^r, p^e))^{|D'(n)|}$$

$$= \prod_{k=e+1}^{r} \phi(p^k)^{|D'(n)|} \det(N(n))$$

$$= \left(\prod_{k=e+1}^{r} \phi(p^k)^{|D'(n)|} \right) \cdot \left(\prod_{d \in D'(n)} \phi(d) \right)$$

$$= \cdot \prod_{k=e+1}^{r} \prod_{d \in D'(n)} \phi(p^k d)$$

$$= \prod_{d \in D_2} \phi(d).$$

So we find

$$\det(M(p^k n, p^e s)) = \left(\prod_{d \in D_1} \phi(d) \right) \left(\prod_{d \in D_2} \phi(d) \right) = \prod_{d \in D} \phi(d).$$

This completes the proof of the determinant formula of $M(a, b)$ by induction on the number of prime factors of b. $\qquad\square$

4.2 Structure of $C_{p^k} \rtimes C_n$

We now perform an explicit calculation for p-hypo-elementary groups before deducing Theorem 4.1.

LEMMA 4.8 *Let G be of the form $C_{p^r} \rtimes C_n$ with $p \nmid n$. Further, let S denote the kernel of the action of C_n on C_{p^r}. Then, for any two subgroups $H', K' \leq G$ of the form $H' = C_{p^e} \rtimes H, K' = C_{p^f} \rtimes K$ with $H, K \leq C_n \leq G$, as elements of the Burnside ring $B(K')$,*

$$\coprod_{g \in H' \backslash G / K'} [H'^g \cap K'] = \frac{|C_n||H \cap K|}{|H||K|} [H' \cap K'] + \frac{p^{r - \max\{e, f\}} |C_n||H \cap K \cap S|}{|H||K|} [H' \cap K' \cap (C_{p^r} \times S)].$$

Proof. First assume $e = f = 0$. Elements of $H\backslash G/K$ are in bijection with H-orbits of cosets gK. For such G, a set of coset representatives of G/K is given by elements $\sigma\tau_i$, where $\sigma \in C_{p^r}$ and $\{\tau_i\}$ are a set of coset representatives of C_n/K. The stabilizer of a right coset gK under the action of H is given by

$$\mathrm{Stab}_H(gK) = H \cap gKg^{-1}.$$

Using that C_n is abelian, for $k \in K$,

$$(\sigma\tau_i)k(\sigma\tau_i)^{-1} = \sigma\tau_i k\tau_i^{-1}\sigma^{-1} = \sigma k\sigma^{-1}$$
$$= \sigma k\sigma^{-1}k^{-1}k = \sigma\varphi(k)(\sigma^{-1})k,$$

where $\varphi\colon C_n \to \mathrm{Aut}(C_{p^r})$ denotes the action of conjugation. Since the prime to p-part of $\mathrm{Aut}(C_{p^r})$ equals that of $\mathrm{Aut}(C_{p^e})$ for any non-trivial $C_{p^e} \leq C_{p^r}$, k acts trivially on $\sigma \neq e$ if and only if $k \in S$. Thus,

$$\sigma\varphi(k)(\sigma^{-1})k \in H \iff k \in H \text{ and } k \in \begin{cases} K & \text{if } \sigma = e \\ K \cap S & \text{if } \sigma \neq e \end{cases}.$$

In particular,

$$\mathrm{Stab}_H(gK) = \begin{cases} H \cap K & \text{if } g \in C_n \\ H \cap K \cap S & \text{if } g \notin C_n \end{cases}.$$

By orbit–stabiliser theorem, there are $\frac{|C_n||H\cap K|}{|H||K|}$ double cosets HgK of length $\frac{|H||K|}{|H\cap K|}$ and $(p^r - 1)\frac{|C_n||H\cap K\cap S|}{|H||K|}$ double cosets of length $\frac{|H||K|}{|H\cap K\cap S|}$. Furthermore, as H has a unique subgroup of each order

$$H^g \cap K = \begin{cases} H \cap K & \text{if } g \in C_n \\ H \cap K \cap S & \text{else} \end{cases},$$

and applying Mackey's formula (1) p7 gives the desired formula in this case.

Now let $e, f \geq 0$. We first calculate the order of $H'\backslash G/K'$. As all p-subgroups of G are normal, there are canonical bijections

$$(C_{p^e} \rtimes H)\backslash G/(C_{p^f} \rtimes K) \leftrightarrow H\backslash G/(C_{p^{\max\{e,f\}}} \rtimes K) \leftrightarrow H\backslash((C_{p^r}/C_{p^{\max\{e,f\}}}) \rtimes C_n)/K.$$

So, from the first part, we find there are $\frac{|C_n||H\cap K|}{|H||K|}$ double cosets of length $\frac{|H||K|}{|H\cap K|}p^{\max\{e,f\}}$ and $(p^{\max\{e,f\}} - 1)\frac{|C_n||H\cap K\cap S|}{|H||K|}$ double cosets of length $\frac{|H||K|}{|H\cap K\cap S|}p^{\max\{e,f\}}$. Taking preimages,

$$H'^g \cap K' = \begin{cases} H' \cap K' & \text{if } g \in C_n \\ H' \cap K' \cap (C_{p^r} \times S) & \text{else} \end{cases}.$$

Therefore, indeed

$$\coprod_{g \in H'\backslash G/K'} [H'^g \cap K'] = \frac{|C_n||H \cap K|}{|H||K|}[H' \cap K'] + \frac{p^{r-\max\{e,f\}}|C_n||H \cap K \cap S|}{|H||K|}[H' \cap K' \cap (C_{p^r} \times S)].$$

$\square$

NOTATION 4.9 Given a group G and subgroup $H \leq G$, we denote by $N_G(H)$ the normaliser of H in G and by $Z_G(H)$ its centraliser.

Proof of Theorem 4.1. Lemma 3.12 states that the permutation pairing for G is non-degenerate if the pairing is non-degenerate for all p-hypo-elementary subgroups. So we shall assume that G is p-hypo-elementary, i.e. $G \cong C_{p^r} \rtimes C_n$ with $p \nmid n$.

For notational convenience, we make a fixed choice of subgroup of G isomorphic to C_n, which we also denote by C_n. Let S denote the kernel of the map $C_n \to \mathrm{Aut}(C_{p^r})$ defining the semi-direct product. Note that S is also the kernel of the map $C_n \to \mathrm{Aut}(C_{p^k})$ for all $1 \leq k \leq r$. Up to conjugacy, any subgroup of G is of the form $C_{p^k} \rtimes L$, with L contained in the fixed choice of C_n. Moreover, such a subgroup is cyclic and normal in G if and only if $L \leq S$.

Let H', K' be non-cyclic subgroups of G. We may assume, by replacing H', K' with conjugate subgroups if necessary, that $H' = C_{p^e} \rtimes H, K' = C_{p^f} \rtimes K$ with $H, K \leq C_n$. We first calculate $\langle H', K' \rangle_{\mathrm{perm}} = v_p(C_{\theta_{H'}}(\mathbb{1}_{K'}\uparrow^G)) = v_p(C_{\theta_{H'}\downarrow_{K'}}(\mathbb{1}_{K'}))$. The decomposition of $\theta_{H'}\downarrow_{K'}$ matches that of its leading term (Lemma 2.16), so applying Lemma 4.8 we find

$$\theta_{H'}\uparrow^G\downarrow_{K'} = \left(\frac{|C_n||H \cap K|}{|H||K|}\right) \cdot \theta_{H' \cap K'}\uparrow^{K'} + \left(\frac{p^{r-\max\{e,f\}}|C_n||H \cap K \cap S|}{|H||K|}\right) \cdot \theta_{H' \cap K' \cap (C_{p^r} \times S)}\uparrow^{K'}.$$

But $H' \cap K' \cap (C_{p^r} \times S)$ is cyclic (so that $\theta_{H' \cap K' \cap (C_{p^r} \times S)} = 0$) and we find

$$v_p(C_{\theta_{H'}}(\mathbb{1}_{K'}\uparrow^G)) = \frac{|C_n||H \cap K|}{|H||K|} v_p(C_{\theta_{H' \cap K'}}(\mathbb{1}_{H' \cap K'})).$$

Let L' be an arbitrary non-cyclic subgroup of the form $C_{p^\ell} \rtimes L$ with $L \leq C_n$. Directly applying (4) to the formula of Example 2.15, or by looking ahead to Example 5.17, we find that

$$v_p(C_{\theta_{L'}}(\mathbb{1}_{L'})) = -\ell\left(1 - \frac{|Z_{L'}(C_{p^\ell})|}{|N_{L'}(C_{p^\ell})|}\right)$$

$$= -\ell\left(1 - \frac{|L \cap S|}{|L|}\right).$$

Concluding our calculation of $\langle H', K' \rangle_{\mathrm{perm}}$, we find

$$\langle H', K' \rangle_{\mathrm{perm}} = \frac{|C_n||H \cap K|}{|H||K|} v_p(C_{\theta_{H' \cap K'}}(\mathbb{1}_{H' \cap K'}))$$

$$= \frac{|C_n||H \cap K|}{|H||K|} \min\{e, f\} \left(\frac{|H \cap K \cap S|}{|H \cap K|} - 1\right)$$

$$= \frac{|C_n|\min\{e, f\}}{|H||K|} (|H \cap K \cap S| - |H \cap K|). \tag{6}$$

Let T be the matrix representing the pairing $\langle\ ,\ \rangle_{\mathrm{perm}}$ with respect to the basis of $P(G)$ given by non-cyclic p-hypo-elementary subgroups ordered (totally in our case) by size. After a non-zero scaling of the rows and columns of T, we obtain a matrix T' with $(H', K')^{\mathrm{th}}$ entry

$$T'_{H', K'} = \min\{e, f\}(|H \cap K \cap S| - |H \cap K|).$$

Note T' remains symmetric and has the same rank as T. Since C_n is cyclic, $|H \cap K \cap S| = \gcd(|H|, |K|, |S|)$ and $|H \cap K| = \gcd(|H|, |K|)$. Thus, T' is the matrix with entries

$$T'_{H', K'} = \min\{e, f\} \left(\gcd(|H|, |K|, |S|) - \gcd(|H|, |K|)\right). \tag{7}$$

Let $M(m, l)$ be as in Notation 4.3. If $Q(d)$ denotes the $d \times d$ matrix with $Q_{i,j} = \min\{i, j\}$, then, by (7), we may simultaneously permute the rows and columns of T' to get

$$T' \sim -Q(r) \otimes M(n, s),$$

where $|S| = s$. As $Q(r)$ is manifestly of full rank and Lemma 4.7 states that $M(n, s)$ is also, so the same is true for T and the permutation pairing for G is non-degenerate. $\square$

EXAMPLE 4.10 Let $G = C_7 \rtimes C_{12}$. A set of representatives of the non-cyclic conjugacy classes of G is given by

$$S := \{C_7 \rtimes C_3, C_7 \rtimes C_4, C_7 \rtimes C_6, C_7 \rtimes C_{12}.\}$$

Applying (6), the matrix T representing the permutation pairing with respect to the basis given by S is given by

$$\begin{pmatrix} -8/3 & 0 & -4/3 & -2/3 \\ 0 & -3/2 & 0 & -1/2 \\ -4/3 & 0 & -4/3 & -2/3 \\ -2/3 & -1/2 & -2/3 & -5/6 \end{pmatrix}.$$

In the notation of the proof of Theorem 4.1, $n = 12$ and $s = 2$. After rescaling the rows and columns of T as in the proof, we obtain the matrix $M(12, 2)$ of Example 4.4.

5 Non-vanishing of the Artin regulator constant

In this section, we prove:

THEOREM 5.1 *For any finite group G and prime p, $v_p(C_{\theta_G}(\mathbb{1}_G)) \neq 0$ if and only if G contains a non-cyclic p-hypo-elementary subgroup. If G does contain a non-cyclic p-hypo-elementary subgroup then $v_p(C_{\theta_G}(\mathbb{1}_G)) \leq -p/|G|$. Here, $\mathbb{1}_G$ denotes the trivial $\mathbb{Z}_p[G]$-module.*

The method of proof is of explicit group theoretic natured and is disjoint to that of Section 4. Moreover, Sections 6 and 7 have no dependency on this section.

REMARK 5.2 The forward direction of Theorem 5.1 is formal: If G contains no non-cyclic p-hypo-elementary groups then all characteristic zero relations are relations in characteristic p (see Lemma 2.22). But the regulator constant of a characteristic p relation has trivial valuation at p when evaluated at any lattice (Lemma 2.30).

REMARK 5.3 Let G be a p-hypo-elementary group. Then, in terms of the permutation pairing of Construction 3.8, the theorem asserts that every entry in the row and column corresponding to G is strictly negative. By Lemma 3.5, the regulator constant pairing is non-degenerate whenever each p-hypo-elementary subgroup of G contains only cyclic proper subgroups, e.g. $G = S_4$. Under the same hypothesis, permutation modules over $\mathbb{Z}_p$ are determined by extension of scalars to $\mathbb{Q}_p$ and regulator constants (Lemma 3.17).

COROLLARY 5.4 *For any finite group G, as a function on $\mathbb{Z}[G]$-modules, the regulator constant associated to the Artin relation θ_H vanishes identically if and only if H is cyclic.*

Proof. For cyclic H, $\theta_H = 0$ so its regulator constant is trivial. For the converse, we first show:

CLAIM *A finite group K is cyclic if and only if all its ℓ-hypo-elementary subgroups are cyclic for all ℓ.*

Proof of Claim. Suppose K is a group for which all its ℓ-hypo-elementary subgroups are cyclic for all ℓ. Then, as the Sylow subgroups must be cyclic, the normaliser of every Sylow subgroup must be equal to its centraliser. Burnside's normal p-complement theorem then ensures that every Sylow p-subgroup normalises every Sylow ℓ-subgroup for $\ell \neq p$. As a result, K is a direct product of its (cyclic) Sylow subgroups for different p, and thus K is cyclic. $\square$

Now suppose $T \leq G$ is non-cyclic. By the claim, T has a non-cyclic ℓ-hypo-elementary subgroup L for some ℓ. Then,

$$
\begin{aligned}
0 \ &\overset{5.1}{>} \ v_\ell(C_{\theta_L}(\mathbb{1}_{\mathbb{Z}_\ell, L})) \\
&\overset{2.16\ i)}{=} \ v_\ell(C_{\theta_T \downarrow_L}(\mathbb{1}_{\mathbb{Z}_\ell, L})) \\
&\overset{2.27\ iv)}{=} \ v_\ell(C_{\theta_T}(\mathbb{1}_{\mathbb{Z}_\ell, L}\uparrow^T)) \\
&\overset{2.27\ vi)}{=} \ v_\ell(C_{\theta_T}(\mathbb{1}_{\mathbb{Z}, L}\uparrow^T)). \qquad \square
\end{aligned}
$$

REMARK 5.5 By symmetry (Lemma 3.9), we find that a permutation module $\mathbb{1}\uparrow^G_H$ is trivial under all regulator constants if and only if H is cyclic.

5.1 Explicit Artin induction

The proof of Theorem 5.1 is made possible by Brauer's formula for explicit Artin induction.

NOTATION 5.6 Let $\mu(n)$ denote the Möbius function of a natural number n,

$$
\mu(n) = \begin{cases} (-1)^r & \text{if } n \text{ is squarefree and has } r \text{ distinct prime factors} \\ 0 & \text{if } n \text{ is not squarefree} \end{cases}.
$$

Note that $\mu(1) = 1$.

LEMMA 5.7 (Brauer, [Sna94, Thm. 2.1.3]) *If G is any finite group and $\theta_G = [G] - \sum_{\mathrm{cyc}(G)} \alpha_H[H]$ is its Artin relation, then*

$$
\alpha_H = \frac{1}{|N_G(H) : H|} \sum_{C \geq H} \mu(|C : H|).
$$

Here the sum runs over all cyclic overgroups of H (not just up to conjugacy).

LEMMA 5.8 *Let G be a p-hypo-elementary group and $\theta_G = [G] - \sum_{\substack{H \leq_G G \\ H \text{ cyclic}}} \alpha_H[H]$. Then $\alpha_H \in \frac{p}{|G|} \cdot \mathbb{Z}$.*

Proof. Let $G = P \rtimes C$ be non-cyclic and $H \leq G$ cyclic. By explicit Artin induction, $\alpha_H \in \frac{1}{|N_G(H):H|} \cdot \mathbb{Z}$, so there is only anything to prove when H is of order coprime to p and H is normalised by P (and so by G). Such an H must therefore lie in the kernel S of the action of C on P.

Let q be the quotient map $q\colon G \to G/H$. Then, a subgroup $K \leq G$ is cyclic if and only if $q(K)$ is. So q defines an index preserving bijection between cyclic subgroups of G containing H and cyclic subgroups of G/H. As such, we may assume that $H = \{1\}$.

We shall show that the contributions to $\sum_{K \text{ cyclic}} \mu(|K|)$ from cyclic subgroups of order coprime to p, and of order divisible by p exactly once, cancel (recall that $\mu(|K|)$ vanishes for all other K). Let K be a cyclic subgroup of G of order coprime to p. We split into two cases: First assume K is normal. Any cyclic group containing K with index p is of the form $C_p \times K$ for some $C_p \leq P$. By (the general form of) Sylow's theorems there are 1 (mod p) such choices. Since $\mu(|C_p \times K|) = -\mu(|K|)$ the contributions of K and its overgroups cancel modulo p.

Now assume that K is not normal. In particular, K is not normalised by P and there are no cyclic subgroups isomorphic to $C_p \times K$. As P acts transitively on the non-singleton set of conjugates of K, orbit-stabiliser shows that the number of subgroups of G isomorphic to K is 0 (mod p). We have exhausted all cyclic subgroups and thus p divides $\sum_{\substack{C \leq G \\ C \text{ cyclic}}} \mu(|C|)$ and $\alpha_H \in \frac{p}{|G|} \cdot \mathbb{Z}$. $\qquad \square$

COROLLARY 5.9 *For any non-cyclic p-hypo-elementary group G and module M, $v_p(C_{\theta_G}(M)) \in \frac{p}{|G|} \cdot \mathbb{Z}$.*
More generally, for any finite group G, given subgroups H, K and a K module M, $v_p(C_{\theta_H}(M\uparrow_K^G)) \in$
$\frac{p}{\gcd\{|H|,|K|\}} \cdot \mathbb{Z}$.

Proof. By definition the valuations of regulator constants of integral Brauer relations lie in $\mathbb{Z}$, so the first statement follows from the lemma and 2.27 *iii)*. For the second, the formalism of Lemma 2.27 and Mackey's formula gives

$$v_p(C_{\theta_H \uparrow_H^G}(M\uparrow_K^G)) = v_p(C_{\theta_H}(M\uparrow_K^G\downarrow_H))$$
$$= \sum_{g \in H \backslash G / K} v_p(C_{\theta_H}(M^g\downarrow_{K^g \cap H}\uparrow^H))$$
$$= \sum_{g \in H \backslash G / K} v_p(C_{\theta_H \downarrow_{K^g \cap H}}(M^g\downarrow_{K^g \cap H})).$$

But applying the first statement, each term of the sum lies in $\frac{p}{\gcd\{|H|,|K|\}} \cdot \mathbb{Z}$. □

We now look to use explicit Artin induction to provide a formula for $v_p(C_{\theta_G}(\mathbb{1}_G))$.

NOTATION 5.10 Recall that if two subgroups H_1, H_2 of G are conjugate, then $[H_1]$ and $[H_2]$ are isomorphic as G-sets. To make the Artin relation slightly more canonical, instead of writing

$$\theta_G = [G] - \sum_{H \leq_G G} \alpha_H [H],$$

we can choose to write θ_G uniquely as

$$\theta_G = [G] - \sum_{H \leq G} \alpha'_H [H],$$

subject to the stipulation that $\alpha'_{H_1} = \alpha'_{H_2}$ for conjugate H_1, H_2. Then $\alpha'_H = \frac{1}{|G:N_G(H)|} \cdot \alpha_H$, the α'_H are unique and the two notational choices denote identical elements of $B(G)$.

NOTATION 5.11 Fix a single prime p for the remainder of this section. Let $\mathcal{P}(G,k)$ denote the number of elements of a given finite group G whose order is divisible by p^k.

LEMMA 5.12 *For any group G and prime p, if θ_G denotes the Artin relation, then*

$$v_p(C_{\theta_G}(\mathbb{1}_G)) = -v_p(|G|) + \frac{1}{|G|} \sum_{g \in G} v_p(|g|) + \frac{\mathcal{P}(G,1)}{|G| \cdot (p-1)}. \tag{8}$$

Proof. Running over all cyclic subgroups rather than their conjugacy classes, explicit Artin induction gives that

$$\theta_G = [G] - \sum_{\substack{H \leq G \\ H\text{-cyclic}}} [H] \cdot \frac{1}{|G:H|} \sum_{\substack{C \geq H \\ C\text{-cyclic}}} \mu(|C:H|).$$

Applying the formula (4) for regulator constants at the trivial module we find that

$$v_p(C_{\theta_G}(\mathbb{1}_G)) = -v_p(|G|) + \sum_{H \leq G} \frac{v_p(|H|)}{|G:H|} \sum_{C \geq H} \mu(|C:H|),$$

26

where from now on it is assumed that sums run only over all cyclic subgroups or overgroups. Changing the order of summation,

$$v_p(C_{\theta_G}(\mathbb{1}_G)) = -v_p(|G|) + \sum_{C \leq G} \sum_{H \leq C} \frac{v_p(|H|)}{|G:H|} \mu(|C:H|)$$

$$= -v_p(|G|) + \sum_{\substack{C \leq G \\ p||C|}} \sum_{H \leq C} \frac{v_p(|H|)}{|G:H|} \mu(|C:H|)$$

as only subgroups C for which p divides $|C|$ make any contribution. Within the second sum, by definition of the Möbius function, only the subgroups of squarefree index contribute. We separate into the sums over the subgroups H of C of index divisible by p, and subgroups H of index not divisible by p. There is a bijection between these two sets given by sending a subgroup H of index not divisible by p to pH. Thus,

$$v_p(C_{\theta_G}(\mathbb{1}_G)) = -v_p(|G|) + \sum_{\substack{C \leq G \\ p||C|}} \sum_{\substack{H \leq C \\ p\nmid|C:H|}} \frac{v_p(|H|)}{|G:H|} \mu(|C:H|) + \sum_{\substack{C \leq G \\ p||C|}} \sum_{\substack{H \leq C \\ p\nmid|C:H|}} \frac{v_p(|pH|)}{|G:pH|} \mu(|C:pH|)$$

$$= -v_p(|G|) + \sum_{\substack{C \leq G \\ p||C|}} \sum_{\substack{H \leq C \\ p\nmid|C:H|}} \frac{v_p(|H|)}{|G:H|} \mu(|C:H|) - \sum_{\substack{C \leq G \\ p||C|}} \sum_{\substack{H \leq C \\ p\nmid|C:H|}} \frac{v_p(|H|) - 1}{p|G:H|} \mu(|C:H|)$$

$$= -v_p(|G|) + \sum_{\substack{C \leq G \\ p||C|}} \sum_{\substack{H \leq C \\ p\nmid|C:H|}} \left(v_p(|H|) \cdot \frac{p-1}{p} \cdot \frac{\mu(|C:H|)}{|G:H|} + \frac{\mu(|C:H|)}{p|G:H|} \right)$$

$$= -v_p(|G|) + \underbrace{\sum_{\substack{C \leq G \\ p||C|}} \sum_{\substack{H \leq C \\ p\nmid|C:H|}} v_p(|H|) \cdot \frac{p-1}{p} \cdot \frac{\mu(|C:H|)}{|G:H|}}_{(\dagger)} + \underbrace{\sum_{\substack{C \leq G \\ p||C|}} \sum_{\substack{H \leq C \\ p\nmid|C:H|}} \frac{\mu(|C:H|)}{p|G:H|}}_{(\star)}$$

We claim that $(\star)$ is equal to $\frac{\mathcal{P}(G,1)}{|G| \cdot (p-1)}$ and $(\dagger)$ is equal to $\frac{1}{|G|} \sum_{g \in G} v_p(|g|)$. To see this suppose that $f \colon G \to \mathbb{C}$ is any map of sets which is constant on elements $g \in G$ for which $v_p(|g|)$ is equal and for which $f(g) = 0$ when $v_p(|g|) = 0$. In this case, we have that

$$\sum_{\substack{C \leq G \\ p||C|}} \sum_{\substack{H \leq C \\ p\nmid|C:H|}} \frac{p-1}{p} \frac{\mu(|C:H|)}{|G:H|} f(h) = \frac{1}{|G|} \sum_{g \in G} f(g),$$

where on the left hand side h denotes any generator of H. This follows from the fact that for a cyclic group C

$$\sum_{H \leq C} \mu(|C:H|)|H| = |\{\text{generators of C}\}|.$$

Setting $f(g) = v_p(|g|)$ gives

$$\sum_{\substack{C \leq G \\ p||C|}} \sum_{\substack{H \leq C \\ p\nmid|C:H|}} v_p(|H|) \cdot \frac{p-1}{p} \cdot \frac{\mu(|C:H|)}{|G:H|} = \frac{1}{|G|} \sum_{g \in G} v_p(|g|),$$

whilst taking $f(g) = \begin{cases} \frac{1}{p-1} & p \mid |g| \\ 0 & p \nmid |g| \end{cases}$ shows that

$$\sum_{\substack{C \leq G \\ p \mid |C|}} \sum_{\substack{H \leq C \\ p \nmid |C:H|}} \frac{\mu(|C:H|)}{p|G:H|} = \frac{1}{|G|} \sum_{\substack{g \in G \\ v_p(|g|) \geq 1}} \frac{1}{p-1}$$

$$= \frac{\mathcal{P}(G,1)}{|G| \cdot (p-1)}.$$

In conclusion,

$$v_p(C_{\theta_G}(\mathbb{1}_G)) = -v_p(|G|) + \frac{1}{|G|} \sum_{g \in G} v_p(|g|) + \frac{\mathcal{P}(G,1)}{|G| \cdot (p-1)}.$$

$\square$

We shall see that the value of (8) is less than or equal to zero for all groups G. Thus, Theorem 5.1 gives a numerical characterisation of groups for which all p-hypo-elementary subgroups are cyclic:

COROLLARY 5.13 *Let G be any finite group and p a prime. Then, G contains no non-cyclic p-hypo-elementary subgroups if and only if*

$$\frac{1}{|G|} \sum_{g \in G} v_p(|g|) + \frac{\mathcal{P}(G,1)}{|G| \cdot (p-1)} = v_p(|G|).$$

The reverse direction whilst a consequence of the argument given in Remark 5.2 is already somewhat non-obvious.

REMARK 5.14 Suppose that G has non-cyclic Sylow p-subgroups. Let $d = v_p(|G|)$, as G contains no elements of order p^d, for any $g \in G$ $v_p(|g|) \leq d-1$ and we may crudely bound

$$\frac{1}{|G|} \sum_{g \in G} v_p(|g|) + \frac{\mathcal{P}(G,1)}{|G| \cdot (p-1)} \leq \frac{1}{|G|} \sum_{g \in G} \left(d-1 + \frac{1}{p-1} \right)$$

$$< d.$$

Applying (8) gives

$$v_p(C_{\theta_G}(\mathbb{1}_G)) < 0.$$

The case of cyclic Sylow p-subgroups requires considerably more care.

5.2 Average p-orders of elements of groups with cyclic Sylow subgroups

In this section, we complete the proof of Theorem 5.1 by explicit calculation of $v_p(C_{\theta_G}(\mathbb{1}_G)))$ for groups with cyclic Sylow p-subgroups using (8) for groups with cyclic Sylow p subgroups. This requires an explicit calculation of $\mathcal{P}(G,k)$ in terms of elementary invariants:

PROPOSITION 5.15 *Let G be any group with cyclic Sylow p-subgroups of order p^r. Then, for any $1 \leq k \leq r$,*

$$\mathcal{P}(G,k) = \left(\frac{p^{r-k+1}-1}{p^{r-k+1}} \right) \frac{|G||Z_G(Q)|}{|N_G(Q)|},$$

where Q denotes any choice of non-trivial p-subgroup of G. If $k = 0$, then $\mathcal{P}(G,k) = |G|$ and if $k > r$, then $\mathcal{P}(G,k) = 0$.

Here, $Z_G(-)$ is as defined in Notation 4.9. We split the proof into four intermediate claims. Firstly, the ratio $|N_G(Q)|/|Z_G(Q)|$ is independent of the choice of Q:

CLAIM 1 *If G is any finite group and p a prime such that G has cyclic Sylow p-subgroups, then, as Q runs over non-trivial p-subgroups, $|N_G(Q)|/|Z_G(Q)|$ is constant.*

Proof. For such a group all p-subgroups of the same order are conjugate. If Q, Q' are conjugate p-subgroups their normalisers and centralisers are related by conjugation and so the above ratio is constant. Thus, we need just show that if P is a subgroup of order p^e, $e \geq 2$, and Q its unique subgroup of order p^{e-1}, then

$$\frac{|N_G(P)|}{|Z_G(P)|} = \frac{|N_G(Q)|}{|Z_G(Q)|}. \tag{9}$$

First note that $N_G(P) \cap Z_G(Q) = Z_G(P)$. This is because both sides contain P, but the coprime to p-part of $\mathrm{Aut}(P)$ is canonically isomorphic to the coprime to p-part of $\mathrm{Aut}(Q)$ (both are cyclic of order $p-1$). In other words, within $N_G(P)$, to centralise Q is to centralise P. As a result, there is an inclusion

$$N_G(P)/Z_G(P) \hookrightarrow N_G(Q)/Z_G(Q),$$

and to prove (9) we must show that $N_G(Q) = N_G(P)Z_G(Q)$. Indeed, as all terms are contained in $N_G(Q)$, we may assume that $Q \trianglelefteq G$. Each choice of subgroup of order p^e (i.e. conjugate of P) must centralise Q, its unique subgroup of order p^{e-1}, thus $\bigcup_{g \in G/N_G(P)} P^g \subseteq Z_G(Q)$. In particular, $Z_G(Q)$ contains a representative of each coset of $G/N_G(P)$ and so $N_G(P)Z_G(Q) = G$. And in general, $N_G(P)Z_G(Q) = N_G(Q)$. $\qquad\square$

Next, we show that to prove the formula for fixed k we may reduce to groups with a central C_{p^k} subgroup.

CLAIM 2 *For any finite group G, prime p and $k \geq 1$, all elements of G of order divisible by p^k are contained in $\bigcup_Q Z_G(Q)$ as Q runs over subgroups of G isomorphic to C_{p^k}. Moreover, if G has cyclic Sylow p-subgroups, then*

$$\mathcal{P}(G, k) = |G : N_G(Q)| \cdot \mathcal{P}(Z_G(Q), k),$$

for any choice of $Q \cong C_{p^k}$.

Proof. Let $g \in G$ and $v_p(|g|) \geq k$. Then, g centralises the subgroup of $\langle g \rangle$ isomorphic to C_{p^k}. So g is contained in $\bigcup_Q Z_G(Q)$, the union of the centralisers of all C_{p^k}-subgroups of G. Now let $Q \leq G$ be some C_{p^k}-subgroup. Since G has cyclic Sylow p-subgroups, Q must be the unique C_{p^k}-subgroup of $Z_G(Q)$. As a result, if Q' is a distinct C_{p^k}-subgroup, then $Z_G(Q) \cap Z_G(Q')$ does not contain any C_{p^k}-subgroup, and so $\mathcal{P}(Z_G(Q) \cap Z_G(Q'), k) = 0$. Thus,

$$\mathcal{P}(G, k) = \sum_Q \mathcal{P}(Z_G(Q), k) = |G : N_G(Q)| \cdot \mathcal{P}(Z_G(Q), k). \qquad\square$$

As a basis for induction we show:

CLAIM 3 *Let G be any group and Q a subgroup of order p that is contained in the centre. Then,*

$$\mathcal{P}(G, 1) = \mathcal{P}(G/Q, 1) + \frac{p-1}{p} \cdot |G|.$$

Proof. Consider the sequence

$$1 \to Q \to G \xrightarrow{q} G/Q \to 1,$$

and let h run over elements of G/Q. First assume that h has order not divisible by p. As $Q \leq Z(G)$, the preimage of $\langle h \rangle$ is isomorphic to $C_p \times C_{|h|}$ on which q is projection onto the second factor. Thus, $q^{-1}(h)$ contains precisely $p - 1$ elements of order p.

Otherwise, if h has order divisible by p, then all elements of $q^{-1}(h)$ have order divisible by p. As a result

$$\mathcal{P}(G, 1) = p \cdot \mathcal{P}(G/Q, 1) + (p - 1)(|G/Q| - \mathcal{P}(G/Q, 1)),$$

giving the stated formula. $\qquad \square$

The inductive step is given by:

CLAIM 4 *Let G be any group with cyclic Sylow p-subgroups and containing a central subgroup Q of order p^k with $k \geq 2$. Then,*

$$\mathcal{P}(G, k) = p \cdot \mathcal{P}(G/\tilde{Q}, k - 1),$$

where $\tilde{Q} \leq Q$ denotes the subgroup of order p

Proof. Consider the sequence

$$1 \to \tilde{Q} \to G \xrightarrow{q} G/\tilde{Q} \to 1.$$

Running over elements $h \in G/\tilde{Q}$, we find that if p^k divides $|h|$, then all p preimages have order divisible by p^k and conversely if $p^{k-1} \nmid |h|$, then none do.

Now assume that p^{k-1} is the maximal power of p dividing $|h|$. Then, $H := q^{-1}(\langle h \rangle)$ is a subgroup of G with Sylow p-subgroups of order p^k. Thus, H must be of the form $C_{p^k} \times A$ with p not dividing the order of A. Via this description q is the quotient $C_{p^k} \times A \to C_{p^k}/C_p \times A$. So, as h has order divisible by p^{k-1}, all elements in the fibre of h have order divisible by p^k. In conclusion,

$$\mathcal{P}(G, k) = p \cdot \mathcal{P}(G/\tilde{Q}, k - 1). \qquad \square$$

Proof of Prop. 5.15. We first show the formula when $k = 1$. The formula trivially holds when $r = 0$. If $r \geq 1$, we may apply Claim 2 to assume that G contains a central subgroup Q isomorphic to C_p. When $r = 1$, the formula is given by Claim 3. Now assume $r \geq 2$. We wish to show that

$$\mathcal{P}(G, 1) = \left(\frac{p^r - 1}{p^r} \right) |G|.$$

Applying Claim 3 and the inductive hypothesis,

$$\mathcal{P}(G, 1) = \mathcal{P}(G/Q, 1) + \left(\frac{p - 1}{p} \right) |G|$$

$$= \left(\frac{p^{r-1} - 1}{p^{r-1}} \right) \frac{|G/Q| \cdot |Z_{G/Q}(Q')|}{|N_{G/Q}(Q')|} + \left(\frac{p - 1}{p} \right) |G|,$$

where Q' is a choice of C_p-subgroup of G/Q. Let P denote the preimage of Q' in G. Recall, for a chain of subgroups $A \geq B \geq C$ with $C \trianglelefteq A$, then $N_A(B)/C \cong N_{A/C}(B/C)$. Moreover if $C \subseteq Z(A)$, then $Z_A(B)/C = Z_{A/C}(B/C)$. Thus, $|G/Q : N_{G/Q}(Q')| = |G : N_G(P)|$ and $|Z_{G/Q}(Q')| = \frac{1}{p} |Z_G(P)|$. So

$$\mathcal{P}(G, 1) = \left(\frac{p^{r-1} - 1}{p^{r-1}} \right) \frac{|G| \cdot |Z_G(P)|}{|N_G(P)| \cdot p} + \left(\frac{p - 1}{p} \right) |G|$$

$$= \left(\frac{p - 1}{p} + \frac{p^{r-1} - 1}{p^r} \right) |G|$$

$$= \left(\frac{p^r - 1}{p^r} \right) |G|$$

as required, where we used the independence asserted in Claim 1 to show

$$\frac{|Z_G(P)|}{|N_G(P)|} = \frac{|Z_G(Q)|}{|N_G(Q)|} = 1.$$

Thus, the formula holds when $k = 1$.

Now assume $k > 1$ and that the formula holds for all groups and indices $\ell < k$. By Claim 2, we are reduced to verifying the formula for groups with a central subgroup Q isomorphic to C_{p^k}.

Fix a subgroup $\tilde{Q} \leq Q$ of order p. Applying Claim 4,

$$\begin{aligned}
\mathcal{P}(G, k) &= p \cdot \mathcal{P}(G/\tilde{Q}, k-1) \\
&= p \left(\frac{p^{(r-1)-(k-1)+1} - 1}{p^{(r-1)-(k-1)+1}} \right) \frac{|G/\tilde{Q}| \cdot |G/\tilde{Q}|}{|G/\tilde{Q}|} \\
&= \left(\frac{p^{r-k+1} - 1}{p^{r-k+1}} \right) |G|
\end{aligned}$$

which is the required formula. □

Proof of Theorem 5.1. By Remarks 5.2 and Corollary 5.9, we need only prove that if G has a non-cyclic p-hypo-elementary subgroup $v_p(C_{\theta_G}(\mathbb{1}_G)) < 0$. Whilst, by Remark 5.14, we may assume G has cyclic Sylow p-subgroups.

Applying Lemma 5.12, we want to show for such G that

$$\frac{1}{|G|} \sum_{g \in G} v_p(|g|) + \frac{\mathcal{P}(G, 1)}{|G| \cdot (p-1)} \leq v_p(|G|),$$

with equality if and only if all p-hypo-elementary subgroups of G are cyclic. Proposition 5.15 shows that if G has Sylow p-subgroups of order p^r, then

$$\sum_{g \in G} v_p(|g|) = \sum_{k=1}^{r} \mathcal{P}(G, k) = \sum_{k=1}^{r} \left(\frac{p^{r-k+1} - 1}{p^{r-k+1}} \right) \frac{|G||Z_G(Q)|}{|N_G(Q)|}$$

and

$$\frac{\mathcal{P}(G, 1)}{(p-1)} = \left(\frac{p^r - 1}{(p-1)p^r} \right) \cdot \frac{|G||Z_G(Q)|}{|N_G(Q)|},$$

where Q denotes any choice of subgroup of G isomorphic to C_p. Thus,

$$\begin{aligned}
\frac{1}{|G|} \sum_{g \in G} v_p(|g|) + \frac{\mathcal{P}(G, 1)}{|G| \cdot (p-1)} &= \left(\left(\sum_{i=1}^{r} \frac{p^{r-i+1} - 1}{p^{r-i+1}} \right) + \frac{p^r - 1}{(p-1)p^r} \right) \frac{|Z_G(Q)|}{|N_G(Q)|} \\
&= \left(\sum_{i=1}^{r} \frac{p^{r-i+1} - 1}{p^{r-i+1}} + \sum_{i=1}^{r} \frac{1}{p^{r-i+1}} \right) \frac{|Z_G(Q)|}{|N_G(Q)|} \\
&= r \cdot \frac{|Z_G(Q)|}{|N_G(Q)|}.
\end{aligned}$$

So that

$$v_p(C_{\theta_G}(\mathbb{1}_G)) = -r \cdot \left(1 - \frac{|Z_G(Q)|}{|N_G(Q)|} \right)$$

whenever G has cyclic Sylow p-subgroups. Finally, note that a group with cyclic Sylow p-subgroups has no non-cyclic p-hypo-elementary groups if and only if all subgroups of order pq with q a prime distinct to p are isomorphic to $C_p \times C_q$. The latter holds if and only if the normaliser of each C_p-subgroup is equal to its centraliser. So indeed $v_p(C_{\theta_G}(\mathbb{1}_G)) < 0 \iff G$ contains a non-cyclic Sylow p-subgroup, otherwise it is zero. $\qquad\square$

It is worth stating that during the proof we derived the following corollary:

COROLLARY 5.16 *For any finite group G and prime p such that the Sylow p-subgroups of G are cyclic,*

$$v_p(C_{\theta_G}(\mathbb{1}_G)) = -r \cdot \left(1 - \frac{|Z_G(Q)|}{|N_G(Q)|}\right).$$

Here Q denotes any choice of non-trivial p-subgroup of G unless $p \nmid |G|$ in which case $Q = \{1\}$ and $v_p(C_{\theta_G}(\mathbb{1}_G)) = 0$.

When G doesn't have cyclic Sylow p-subgroups, we can only say that $v_p(C_{\theta_G}(\mathbb{1}_G)) \le -\frac{p}{|G|}$.

EXAMPLE 5.17 Let G be a p-hypo-elementary group with a non-trivial cyclic Sylow p-subgroup. Then G is of the form $C_{p^r} \rtimes C_n$ with $(p, n) = 1$. Let S denote the kernel of the map $C_n \to \operatorname{Aut}(C_{p^r})$ defining the semi-direct product and $s = |S|$. Then,

$$v_p(C_{\theta_G}(\mathbb{1}_G)) = -r(1 - \frac{s}{n}),$$

as the centraliser of C_{p^r} is $C_{p^r} \times S \le G$ (the action is trivial) and $C_{p^r} \trianglelefteq G$.

We can also verify this directly. In Example, 2.15 we saw that the Artin relation of such a G is given by

$$\theta_G = [C_{p^r} \rtimes C_n] - [C_n] + \frac{s}{n}[S] - \frac{s}{n}[C_{p^r} \times S].$$

So applying formula (4)

$$C_{\theta_G}(\mathbb{1}_G) = \frac{\left(\frac{1}{|G|}\right) \cdot \left(\frac{1}{|S|}\right)^{\frac{s}{n}}}{\left(\frac{1}{|C_n|}\right)\left(\frac{1}{|C_{p^r} \times S|}\right)^{\frac{s}{n}}},$$

so that indeed

$$v_p(C_{\theta_G}(\mathbb{1}_G)) = -r + \frac{s}{n} \cdot r.$$

6 Yakovlev's theorem and the permutation pairing

If a group G has cyclic Sylow p-subgroups, then Theorem 4.1 shows that the permutation pairing is non-degenerate. As an application, if G is in addition abelian, dihedral, or more generally satisfies the conditions of Theorem 6.8, then we exhibit an explicit list of invariants which determine the isomorphism class of an arbitrary rationally self-dual $\mathbb{Z}_p[G]$-lattice. This requires also understanding the theory over $\mathbb{Z}_{(p)}$, which is somewhat less well behaved.

6.1 Trivial source modules

As we shall see, existing work reduces us to dealing with *trivial source modules*, which we now introduce.

DEFINITION 6.1 For any finite G, we say that an $\mathcal{R}[G]$-module has *trivial source*, or is a *trivial source module*, if it is a direct summand of a permutation module. In other sources, trivial source modules may be referred to as any of relatively projective, permutation projective, p-permutation or invertible. For $\mathcal{R}$ any ring, we denote the subalgebra of $A(\mathcal{R}[G])$ generated by the trivial source modules by $A(\mathcal{R}[G], \mathrm{triv})$.

Our definition is slightly non-standard (cf. [Ben98, Def. 3.11.1]). When $\mathcal{R} = \mathbb{Z}_p$, it coincides with the usual definition [Ben98, Lem. 3.11.2], but when $\mathcal{R} = \mathbb{Z}_{(p)}$, due to the failure of Krull-Schmidt [Ben06], decomposition by vertices fails (see Example 6.19) and what we call an indecomposable trivial source module over $\mathbb{Z}_{(p)}$ need not have source which is trivial. However, in our definition, for M over $\mathbb{Z}_{(p)}$, M is a trivial source module if and only if $M \otimes \mathbb{Z}_p$ is a trivial source module.

EXAMPLE 6.2 Let $\mathcal{R} = \mathbb{Z}_{(p)}$ and $G = C_p$. Up to isomorphism, there are 3 indecomposable $\mathbb{Z}_{(p)}[C_p]$-lattices
$$\mathbb{1}_G, I_G, \mathbb{Z}_{(p)}[C_p],$$
the trivial module, the augmentation ideal of $\mathbb{Z}_{(p)}[C_p]$, and the regular representation [HR62, Thm. 2.6]. The indecomposable trivial source modules are the summands of $\mathbb{1}_{\{1\}}\uparrow^{C_p} \cong \mathbb{Z}_{(p)}[C_p]$ and $\mathbb{1}_{C_p}\uparrow^{C_p} = \mathbb{1}_{C_p}$. So the trivial source indecomposables are precisely $\mathbb{1}_G$ and $\mathbb{Z}_{(p)}[C_p]$, and $A(\mathbb{Z}_{(p)}[G], \mathrm{triv}) = A(\mathbb{Z}_{(p)}[G], \mathrm{perm})$ is two dimensional. The same holds for $\mathcal{R} = \mathbb{Z}_p$.

DEFINITION 6.3 Let M be any $\mathbb{Z}_p[G]$-lattice. We define M_{triv} to be the submodule generated by all indecomposable trivial source summands of M. We call M_{triv} the *trivial source part* of M and call the submodule M_{nt} generated by the indecomposable summands which are not trivial source summands the *non-trivial source part*. By the Krull-Schmidt property of $\mathbb{Z}_p[G]$-modules, we obtain the *trivial source decomposition* $M = M_{\mathrm{triv}} \oplus M_{\mathrm{nt}}$.

REMARK 6.4 Over $\mathbb{Z}_{(p)}$, lattices do not admit unique decomposition [Ben06] and there is no general analogue of the trivial source decomposition. In particular, for M over $\mathbb{Z}_{(p)}$, the trivial source decomposition of $M \otimes \mathbb{Z}_p$ need not be defined over $\mathbb{Z}_{(p)}$. This occurs for the group $C_3 \times C_4$ when $p = 3$ (see [Tor18, Ch. 2]).

6.2 Yakovlev's result

Now assume that G has cyclic Sylow p-subgroups.

NOTATION 6.5 Let P be a choice of Sylow p-subgroup of G. Let r be such that $P \cong C_{p^r}$, and for $0 \leq i \leq r$, let $P_i \leq P$ denote the subgroup of order p^i.

Note that for a $\mathbb{Z}_p[G]$-lattice M, $H^1(P_i, M)$ is a $N_G(P_i)$-module.

THEOREM 6.6 (Yakovlev [Yak96, Thm. 2.1]) *Let G be a finite group and p a prime such that G has cyclic Sylow p-subgroups. If M is a $\mathbb{Z}_p[G]$-lattice, then the isomorphism class of M_{nt} is determined by the following diagram,*

$$H^1(P_r, M) \underset{\mathrm{cores}}{\overset{\mathrm{res}}{\rightleftarrows}} H^1(P_{r-1}, M) \underset{\mathrm{cores}}{\overset{\mathrm{res}}{\rightleftarrows}} \quad ... \quad \underset{\mathrm{cores}}{\overset{\mathrm{res}}{\rightleftarrows}} H^1(P_0, M).$$

Figure 1: Yakovlev diagram

To be precise, when we say "determined by" we mean that, if M' is another $\mathbb{Z}_p[G]$-lattice for which there are $\mathbb{Z}_p[N_G(P_i)]$-module isomorphisms $\kappa_i : H^1(P_i, M) \to H^1(P_i, M'), 0 \leq i \leq n$ which commute with restriction and corestriction in the above diagram, then $M_{\mathrm{nt}} \cong M'_{\mathrm{nt}}$.

CONSTRUCTION 6.7 Call any diagram of the form

$$\bullet \; \underset{b_r}{\overset{a_r}{\underset{\longleftarrow}{\longrightarrow}}} \; \bullet \; \underset{b_{r-1}}{\overset{a_{r-1}}{\underset{\longleftarrow}{\longrightarrow}}} \quad \dots \quad \underset{b_1}{\overset{a_1}{\underset{\longleftarrow}{\longrightarrow}}} \; \bullet,$$

with the ith term a finite $N_G(P_{r-i+1})$-module and a_i, b_i homomorphisms of abelian groups, a *Yakovlev diagram*. For any M, Figure 1 is of this form and we refer to it as the *Yakovlev diagram of M*.

There is an obvious notion of direct sum of such diagrams. Let $\mathcal{C}$ denote the free $\mathbb{Q}$-vector space on isomorphism classes of such diagrams subject to identifying addition of diagrams with addition of elements of $\mathcal{C}$. Taking Yakovlev diagrams defines a canonical map

$$\mathrm{Yak} \colon A(\mathbb{Z}_p[G]) \to \mathcal{C}.$$

Yakovlev's theorem is now the assertion that $\ker(\mathrm{Yak}) = A(\mathbb{Z}_p[G], \mathrm{triv})$. Yakovlev also gives a converse describing which Yakovlev diagrams arise as the cohomology of $\mathbb{Z}_p[G]$-lattices, but we do not need this.

Recall that $A(\mathbb{Z}_{(p)}[G], \mathrm{perm}) = A(\mathbb{Z}_p[G], \mathrm{perm})$ as subspaces of $A(\mathbb{Z}_p[G])$. We are now able to correctly formulate the theorem outlined in the introduction:

THEOREM 6.8 *Let G be any finite group and p a prime such that G has cyclic Sylow p-subgroups and for which $A(\mathbb{Z}_p[G], \mathrm{perm}) = A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$. Then, the isomorphism class of any rationally self-dual $\mathbb{Z}_p[G]$-lattice M is determined by*

i) *the isomorphism class of $M \otimes \mathbb{Q}_p$ as a $\mathbb{Q}_p[G]$-module,*

ii) *the valuations $v_p(C_{\theta_H}(M))$ of the regulator constants of the Artin relations for $H \in \mathrm{nchyp}_p(G)$,*

iii) *the Yakovlev diagram*

$$H^1(P_r, M) \; \underset{\mathrm{cores}}{\overset{\mathrm{res}}{\underset{\longleftarrow}{\longrightarrow}}} \; H^1(P_{r-1}, M) \; \underset{\mathrm{cores}}{\overset{\mathrm{res}}{\underset{\longleftarrow}{\longrightarrow}}} \quad \dots \quad \underset{\mathrm{cores}}{\overset{\mathrm{res}}{\underset{\longleftarrow}{\longrightarrow}}} \; H^1(P_0, M).$$

Proof. By Theorem 6.6 the data of *iii)* determines the isomorphism class of M_{nt}. Now fix some trivial source $\mathbb{Z}_p[G]$-module M' such that $M_{\mathrm{nt}} \oplus M'$ is rationally self-dual. Such an M' exists as M_{triv} is an example. By linearity of regulator constants and extension of scalars, from *i),ii),iii)* we also obtain the regulator constants and isomorphism class of the extension of scalars of $t := [M] - [M_{\mathrm{nt}}] - [M']$ (note that t is rationally self-dual so that its regulator constants are defined). By construction $t \in \ker(\mathrm{Yak} \colon A(\mathbb{Z}_p[G]) \to \mathcal{C}) = A(\mathbb{Z}_p[G], \mathrm{triv})$. It suffices to show that any rationally self-dual element $t \in A(\mathbb{Z}_p[G], \mathrm{triv})$ is determined by the data of *i),ii)*.

Let M'' be any trivial source $\mathbb{Z}_p[G]$-module such that $t - M''$ has rational character, again such an M'' certainly exists. Now, any $\mathbb{Z}_p[G]$-lattice N for which $N \otimes \mathbb{Q}_p$ is defined over $\mathbb{Q}$ is the extension of scalars of a $\mathbb{Z}_{(p)}[G]$-lattice [Rei70, Prop. 5.7]. As a result, any element of $A(\mathbb{Z}_p[G])$ with rational character is contained within $A(\mathbb{Z}_{(p)}[G])$. In particular, $t - M'' \in A(\mathbb{Z}_p[G], \mathrm{triv}) \cap A(\mathbb{Z}_{(p)}[G])$. We claim that this space is precisely $A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$, so let W, V be trivial source $\mathbb{Z}_p[G]$-modules and assume that $[W] - [V]$ has rational character. If V is a summand of some permutation module T with complement V', then $[W \oplus V'] - [T] = [W] - [V]$ and $W \oplus V'$ is a trivial source module with rational character. So, by [Rei70, Prop. 5.7], $[W] - [V']$ lies in $A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$.

Thus, $t - M'' \in A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$ and so by assumption lies in $A(\mathbb{Z}_p[G], \mathrm{perm})$. As a result, it is determined by its regulator constants and extension of scalars (Corollary 4.2). Tracing back, we find that M is determined by the data of *i),ii),iii)*. $\qquad \square$

Since *i),ii),iii)* are isomorphism invariants, two $\mathbb{Z}_p[G]$-lattices are isomorphic if and only if *i),ii),iii)* are the same for both lattices.

REMARK 6.9 The restriction on being rationally self-dual is a somewhat mild one. For example, if M_1, M_2 are any two $\mathbb{Z}_p[G]$-lattices, then $M_1 \cong M_2$ if and only if, *i),iii)* of Theorem 6.8 coincide for M_1, M_2 and

ii') there exists some $\mathbb{Z}_p[G]$-lattice N such that $M_1 \oplus N$ and $M_2 \oplus N$ are both rationally self-dual, and the valuations $v_p(C_{\theta_H}(M_i \oplus N))$ of the regulator constants of the Artin relations of $M_i \oplus N$ are equal for all $H \in \mathrm{nchyp}_p(G)$.

Note, it is easy to determine if there exists a $\mathbb{Z}_p[G]$-lattice N such that $M_1 \oplus N$ and $M_2 \oplus N$ are rationally self-dual using *i)*. If the $v_p(C_{\theta_H}(M_i \oplus N))$ are equal for one such N, then they are equal for all.

The condition that $A(\mathbb{Z}_p[G], \mathrm{perm}) = A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$ is investigated in the next subsection. For reference, we shall see that the equality can be checked on restriction to the p-hypo-elementary subgroups and that dihedral groups, abelian groups with cyclic Sylow p-subgroups and groups of order coprime to $p-1$ all have this property, but $C_p \rtimes C_{p-1}$ for $p \geq 5$ does not. In Section 7.1, we provide a worked example of Theorem 6.8 for dihedral groups of order $2p$ with p odd.

REMARK 6.10 Theorem 6.8 is sharp in the following sense. If $A(\mathbb{Z}_p[G], \mathrm{perm}) \subsetneq A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$ or the permutation pairing is degenerate, then rationally self-dual $\mathbb{Z}_p[G]$-lattices are not determined by *i),ii),iii)*. The first case can be seen by comparing the dimension of $A(\mathbb{Z}_p[G], \mathrm{triv})$ and the maximum number of linear conditions on elements of $A(\mathbb{Z}_p[G], \mathrm{triv})$ we could possibly obtain from *i),ii)* using Lemmas 6.24, 6.25 and the formulae of Section 2.4. In the second case, not even all permutation lattices can be distinguished (see Lemma 3.17).

6.3 Species and trivial source modules over $\mathbb{Z}_{(p)}$

Now let G be any finite group.

DEFINITION 6.11 A *species*[1] is a ring homomorphism $A(\mathbb{Z}_p[G], \mathrm{triv}) \to \mathbb{C}$.

EXAMPLE 6.12 For any $g \in G$, $\mathrm{tr}(g \mid -)$ defines a ring homomorphism $A(\mathbb{Z}_p[G]) \to \mathbb{C}$ and so also a species.

DEFINITION 6.13 For H a subgroup of G, we say that an indecomposable trivial source $\mathbb{Z}_p[G]$-lattice M has vertex H if M is a direct summand of $\mathbb{1}\uparrow_H^G$ but not of $\mathbb{1}\uparrow_{H'}^G$ for any $H' \lneq H$. The vertices of M form a conjugacy class of subgroups and only p-groups appear as vertices [Ben98, Prop. 3.10.2]. For an arbitrary $\mathbb{Z}_p[G]$-lattice M, we call the summand generated by the indecomposables with vertex P the *vertex P summand* of M, in this way we obtain a decomposition of M indexed by vertices.

CONSTRUCTION 6.14 Consider pairs (P, g), where $P \leq G$ is a p-group and g an element of $N_G(P)$ of order coprime to p, up to simultaneous conjugacy. Then $H := \langle P, g \rangle$ is p-hypo-elementary and to any such pair we may associate a species $t_{(P,g)}$ as follows. Consider the composite

$$A(\mathbb{Z}_p[G], \mathrm{triv}) \to A(\mathbb{Z}_p[H], \mathrm{triv}) \to A(\mathbb{Z}_p[H/P], \mathrm{triv}).$$

---

[1]It is more common to define a species as a ring homomorphism from the trivial source ring over the ring of integers of a sufficiently large extension of $\mathbb{Q}_p$, but this is not necessary for our purposes.

Here the first map is restriction. The second map sends a lattice M to its vertex P summand N, which, as M is trivial source, is inflated from H/P so can be considered as an H/P-module. We define $t_{(P,g)} \colon A(\mathbb{Z}_p[G], \mathrm{triv}) \to \mathbb{C}$ to be the postcomposition with $\mathrm{tr}(g \mid -)$, i.e. $t_{(P,g)}(M)$ is the trace of g acting on N.

EXAMPLE 6.15 For any $g \in G$, the species defined by $\mathrm{tr}(g \mid -)$ is equal to $t_{(P,g^{|g|})}$, where $|P|$ is the Sylow p-subgroup of $\langle g \rangle$.

The $t_{(P,g)}$ need not be distinct, but all species arise in this way:

THEOREM 6.16 (Conlon) *For any finite group G and prime p, there is an inclusion*

$$\prod t_{(P,g)} \colon A(\mathbb{Z}_p[G], \mathrm{triv}) \to \prod_{(P,g)} \mathbb{C}.$$

Proof. This is usually stated for the ring of integers $\mathcal{O}_K$ of a sufficiently large extension $K/\mathbb{Q}_p$ (see [Ben98, Cor. 5.5.5]). The stated version then follows as, for $K/\mathbb{Q}_p$ and M, M' any $\mathbb{Z}_p[G]$-lattices, $M \cong M' \iff (M \otimes \mathcal{O}_K) \cong (M' \otimes \mathcal{O}_K)$ and that the action of Galois ensures vertices are preserved under base change by $\mathcal{O}_K/\mathbb{Z}_p$. ∎

REMARK 6.17 It is worth remarking that although species are good invariants of trivial source modules they cannot be combined with Yakovlev diagrams to give results such as Theorem 6.8. This is because species cannot be canonically extended beyond $A(\mathbb{Z}_p[G], \mathrm{triv})$. On the other hand, regulator constants are defined for an arbitrary rationally self-dual lattice.

LEMMA 6.18 *For a permutation module $\mathbb{1}_K{\uparrow}^G$, we find $t_{(P,g)}(\mathbb{1}_K{\uparrow}^G) = \#(G/K)^H$, where $H = \langle P, g \rangle$.*

Proof. By definition $t_{(P,g)}$ is a function of $\mathbb{1}_K{\uparrow}^G{\downarrow}_H = \bigoplus_{K \backslash G / H} \mathbb{1}{\uparrow}^H_{K^g \cap H}$. We claim that only the terms with $K^g \cap H = H$ have non-trivial species. Indeed, if $K^g \cap H \not\geq P$, then the vertex P summand of $\mathbb{1}{\uparrow}^H_{K^g \cap H}$ is zero, whilst if $K^g \cap H \geq P$, then $\mathbb{1}{\uparrow}^H_{K^g \cap H}$ is all of vertex P and is inflated from the quotient $\langle g \rangle$. It is then clear that $\mathrm{tr}(g \mid -)$ is zero if and only if $K^g \cap H \neq H$, else it is one.

Finally, the number of elements of $K \backslash G / H$ with $K^g \cap H = H$ is precisely the number of elements of G/K fixed under H. ∎

EXAMPLE 6.19 It is not the case that the species of a trivial source lattice M over $\mathbb{Z}_{(p)}$ need take only rational values. This is made possible by the failure of Krull-Schmidt over $\mathbb{Z}_{(p)}$. For example, if $p \geq 5$ and $G = C_p \rtimes C_{p-1}$ with C_{p-1} acting faithfully, then a trivial source module with non-rational species is constructed as follows (cf. [Ben06]). Let χ denote the inflation of a faithful character of C_{p-1}. The trivial source $\mathbb{Z}_p[G]$-modules are then the summands of

$$\mathbb{1}{\uparrow}^G = \bigoplus_{i=0}^{p-2} \mathbb{1}{\uparrow}^G_{C_{p-1}} \otimes \chi^i,$$

$$\mathbb{1}{\uparrow}^G_{C_p} = \bigoplus_{i=0}^{p-2} \chi^i.$$

Then,

$$M := \left(\bigoplus_{\substack{i=0 \\ i \neq 1}}^{p-2} \mathbb{1}{\uparrow}^G_{C_{p-1}} \otimes \chi^i \right) \oplus \chi$$

is defined over $\mathbb{Z}_{(p)}$, but as the only summand of vertex C_p is χ, the vertex decomposition is not defined over $\mathbb{Z}_{(p)}$, and the species of M are non-rational, as $t_{(C_p,\tau)}(M) = \chi(\tau)$ is a primitive $(p-1)^{\text{st}}$ root of unity.

In particular, $A(\mathbb{Z}_p[G], \mathrm{perm}) \subsetneq A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$ as the species of permutation modules are integers (Lemma 6.18).

THEOREM 6.20 *A basis of* $A(\mathbb{Z}_p[G], \mathrm{perm})$ *is given by* $\{\mathbb{1}{\uparrow}_H^G\}_{H \in \mathrm{hyp}_p(G)}$.

Proof. We first check linear independence. By Theorem 6.16, we need only check linear independence after taking species. By Lemma 6.18, the species $t_{(P,g)}(\mathbb{1}{\uparrow}_H^G)$ is zero whenever no conjugate of H contains $\langle P, g \rangle$, whilst $t_{(P,g)}(\mathbb{1}{\uparrow}_{\langle P,g \rangle}^G) \neq 0$. After (non-uniquely) ordering the elements of $\mathrm{hyp}_p(G)$ by increasing size, linear independence is now clear.

Now, let i be such that $\langle P, g \rangle = \langle P, g^i \rangle$ and let $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ raise the $|g|^{\text{th}}$ roots of unity to the ith power. Then, for any trivial source module M over $\mathbb{Z}_p$,

$$
\begin{aligned}
t_{(P,g^i)}(M) &= \mathrm{tr}(g^i \mid \text{vertex } P \text{ summand of } M{\downarrow}_{\langle P,g^i \rangle}) \\
&= \mathrm{tr}(g^i \mid \text{vertex } P \text{ summand of } M{\downarrow}_{\langle P,g \rangle}) \\
&= \mathrm{tr}(g \mid \text{vertex } P \text{ summand of } M{\downarrow}_{\langle P,g \rangle})^\sigma \\
&= t_{(P,g)}(M)^\sigma.
\end{aligned}
$$

But for permutation modules M, $t_{(P,g)}(M)$ is rational (Lemma 6.18), so $t_{(P,g)}(M)$ is constant on pairs (P, g) generating the same p-hypo-elementary subgroup up to conjugacy. Therefore, $\dim_{\mathbb{Q}} A(\mathbb{Z}_p[G], \mathrm{perm}) \leq \#\{\text{conjugacy classes of } p\text{-hypo-elementary groups}\}$. □

We used this in Theorem 2.20 to find a basis of the space of Brauer relations in characteristic p. Examining the proof of the theorem we find:

COROLLARY 6.21 *For any finite group G and prime p, $A(\mathbb{Z}_p[G], \mathrm{perm}) \subseteq A(\mathbb{Z}_p[G], \mathrm{triv})$ is precisely the subspace of elements whose species are all rational.*

This also follows from work of Fan Yun [Fan91].

LEMMA 6.22 *Let G be a finite group and p a prime. If $A(\mathbb{Z}_p[H], \mathrm{perm}) = A(\mathbb{Z}_{(p)}[H], \mathrm{triv})$ for all $H \in \mathrm{hyp}_p(G)$, then $A(\mathbb{Z}_p[G], \mathrm{perm}) = A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$.*

Proof. Suppose that $a \in A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$ is such that, upon restriction to every p-hypo-elementary subgroup H, $a{\downarrow}_H$ is a permutation module. Then $a{\downarrow}_H$ has rational species (Lemma 6.18). But then a itself must have rational species as species are defined via restriction to the p-hypo-elementary subgroups. Applying Corollary 6.21 we find $a \in A(\mathbb{Z}_{(p)}[G], \mathrm{perm})$. □

As a result, a group G satisfies the conditions of Theorem 6.8 if its p-hypo-elementary subgroups do.

NOTATION 6.23 Let $(P, g), (P', g')$ define two species and set $n = |g|$. We say $(P, g) \sim_p (P', g')$ if there exists an element $h \in G$ such that $(P')^h = P$ and $(g')^h = g^i$ for some $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ with $i \equiv 1$ (mod $\gcd(n, p-1)$).

LEMMA 6.24 *For any finite group G and prime p,*

  i) $\dim(A(\mathbb{Z}_p[G], \mathrm{triv})) = \#(\{\text{species } (P, g)\}/\sim_p)$,

ii) $\dim(\mathrm{im}(A(\mathbb{Z}_p[G], \mathrm{triv}) \to A(\mathbb{Q}_p[G]))) = \#(\{species\ (P, g)\ |\ \langle P, g\rangle\ is\ cyclic\}/\sim_p).$

Proof. For any finite Galois extension $K/\mathbb{Q}_p$, the action of $\mathrm{Gal}(K/\mathbb{Q}_p)$ on lattices respects decompositions into vertices. As a result, $t_{(P,g)}(-) = t_{(P,g^i)}(-)$ as functions on $A(\mathbb{Z}_p[G], \mathrm{triv})$ for any integer i such that $(-)^i$ is an automorphism of $\langle g\rangle$ which acts trivially on the subgroup of order $m = \gcd(n, p-1)$, i.e. whenever $(P, g) \sim_p (P, g^i)$. Together with Theorem 6.16, this demonstrates the upper bound on $\dim A(\mathbb{Z}_p[G], \mathrm{triv})$. For the lower bound, use that the Green correspondence provides a distinct indecomposable trivial source module of vertex P for every projective indecomposable $\mathbb{Z}_{(p)}[N_G(P)/P]$-lattice (see e.g. [Ben98, Thm. 3.12.2]), of which there are $\#(\{species\ (Q, h)\ |\ Q = P\}/\sim_p)$.

We now show *ii)*. The dimension of $A(\mathbb{Q}_p[G])$ is equal to the number of distinct ring homomorphisms $\mathrm{tr}(g\ |\ -)\colon A(\mathbb{Q}_p[G]) \to \mathbb{C}$. The dimension of $\mathrm{im}(A(\mathbb{Z}_p[G], \mathrm{triv}) \to A(\mathbb{Q}_p[G]))$ is then the number of species up to $\sim_p$ which are of the form $\mathrm{tr}(g\ |\ -)$. By Example 6.15, this is equal to $\#(\{species\ (P, g)\ |\ \langle P, g\rangle\ is\ cyclic\}/\sim_p)$. □

LEMMA 6.25 *The following are equivalent*

i) $A(\mathbb{Z}_p[G], \mathrm{perm}) = A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$,

ii) *the species of all trivial source $\mathbb{Z}_{(p)}[G]$-lattices are rational,*

iii) *there is an equality*

$$\dim(A(\mathbb{Z}_p[G], \mathrm{perm})) = \dim(A(\mathbb{Z}_p[G], \mathrm{triv}))$$
$$- \dim(\mathrm{im}(A(\mathbb{Z}_p[G], \mathrm{triv}) \to A(\mathbb{Q}_p[G])))$$
$$+ \dim(A(\mathbb{Q}[G])),$$

iv) *there is an equality*

$$\#(\{p\text{-}hypo\text{-}elementary\ subgroups\}/\sim) = \#(\{species\ (P, g)\}/\sim_p)$$
$$- \#(\{species\ (P, g)\ |\ \langle P, g\rangle\ is\ cyclic\}/\sim_p)$$
$$+ \#(\{cyclic\ subgroups\}/\sim),$$

where $\sim$ denotes up to conjugacy.

Proof. The equivalence *i)* $\iff$ *ii)* is Corollary 6.21. For *i)* $\iff$ *iii)*, use that a trivial source $\mathbb{Z}_p[G]$-module is defined over $\mathbb{Z}_{(p)}$ if and only if it has rational character [Rei70, Prop. 5.7], together with the fact that $A(\mathbb{Z}_{(p)}[G], \mathrm{triv}) \to A(\mathbb{Q}[G])$ is surjective by Artin's induction theorem. For *iii)* $\iff$ *iv)*, combine Lemma 6.24, Theorem 6.20 and Artin's induction theorem. □

We conclude by giving examples of groups satisfying the condition $A(\mathbb{Z}_p[G], \mathrm{perm}) = A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$:

EXAMPLE 6.26 If G is abelian with cyclic Sylow p-subgroups, then all p-hypo-elementary subgroups are cyclic and so, by Lemma 6.25 *iv)*, $A(\mathbb{Z}_p[G], \mathrm{perm}) = A(\mathbb{Z}_{(p)}[G], \mathrm{triv})$ (note, there may be $\mathbb{Z}_{(p)}[G]$-lattices M for which $(M \otimes \mathbb{Z}_p)_{\mathrm{triv}}$ does not lie in $A(\mathbb{Z}_p[G], \mathrm{perm})$, see the example of $C_3 \times C_4$ in [Tor18, Ch. 2]). When applying Theorem 6.8 for such G, the fact that there are no non-cyclic p-hypo-elementary subgroups makes the data of *ii)* empty.

EXAMPLE 6.27 Let p be odd and $G = D_{2q}$ be the dihedral group of order $2q$ for any $q \geq 1$. Recall, that we need only check that the condition for all p-hypo-elementary subgroups. The only possible p-hypo-elementary subgroups of G are either cyclic, in which case they are covered by the previous example, or of the form D_{2p^r} for some $r \geq 1$. In that case, species up to $\sim_p$ are in bijection with subgroups and so Lemma 6.25 *iv)* holds.

EXAMPLE 6.28 If $(|G|, p-1) = 1$, then all species of trivial source $\mathbb{Z}_p[G]$-lattices are rational and so by Corollary 6.21, $A(\mathbb{Z}_p[G], \text{perm}) = A(\mathbb{Z}_p[G], \text{triv})$. In particular, when $p = 2$ all groups with cyclic Sylow 2-subgroups satisfy the conditions of Theorem 6.8.

7 Examples

7.1 D_{2p}

Let $G = D_{2p} = C_p \rtimes C_2$ be the dihedral group of order $2p$ for p an odd prime. Then, G satisfies the conditions of Theorem 6.8 for all primes ℓ, by Example 6.27. Since all complex irreducible representations of D_{2p} are defined over $\mathbb{R}$, all $\mathbb{Z}_\ell[G]$-lattices are rationally self-dual for any ℓ.

In this section, we explicate how Theorem 6.8 distinguishes $\mathbb{Z}_\ell[D_{2p}]$-lattices. Broadly, there are three different cases, when $\ell = 2, p$ or when ℓ is coprime to the order of the group. In the latter case character theory applies and we shall for simplicity additionally assume that ℓ is chosen so that all $\mathbb{Q}_\ell[G]$-representations are defined over $\mathbb{Q}[G]$. For example, this is the case if ℓ is a primitive element modulo p.

It is only possible to go into such detail for groups of the form D_{2p} as they are one of the few families of groups for which the isomorphism classes of all indecomposable $\mathbb{Z}_\ell[G]$-lattices have been classified for all ℓ dividing $|G|$.

By assumption all $\mathbb{Q}_\ell[G]$-representations are defined over $\mathbb{Q}$, so by [Rei70, Prop. 5.7] all $\mathbb{Z}_\ell[G]$-lattices are defined over $\mathbb{Z}_{(\ell)}[G]$. In Example 6.27, we checked that $A(\mathbb{Z}_\ell[G], \text{perm}) = A(\mathbb{Z}_{(\ell)}[G], \text{triv})$ for all primes ℓ. So, as in Example 2.23, a basis of $A(\mathbb{Z}_\ell[G], \text{perm}) = A(\mathbb{Z}_{(\ell)}[G], \text{triv})$ is given by

$$S = \begin{cases} \mathbb{1}_{\{1\}}{\uparrow}^G, \mathbb{1}_{C_2}{\uparrow}^G, \mathbb{1}_{C_p}{\uparrow}^G & \ell \neq p \\ \mathbb{1}_{\{1\}}{\uparrow}^G, \mathbb{1}_{C_2}{\uparrow}^G, \mathbb{1}_{C_p}{\uparrow}^G, \mathbb{1}_G & \ell = p \end{cases},$$

and this is also a basis of $A(\mathbb{Z}_\ell[G], \text{triv})$. When $\ell \neq 2$ or p, all $\mathbb{Z}_\ell[G]$-lattices are projective so S forms a basis of $A(\mathbb{Z}_\ell[G])$.

We can exhaust the non-trivial source modules via Yakovlev's theorem (Thm. 6.6). When $\ell = 2$, as $N_{D_{2p}}(C_2) = C_2$, the Yakovlev diagram for a module M simply consists of $H^1(C_2, M)$ as an abelian group. So any $\mathbb{Z}_2[G]$-lattice M for which $H^1(C_2, M) \cong \mathbb{Z}/2\mathbb{Z}$ will extend S to a basis of $A(\mathbb{Z}_2[G])$. The sign representation ϵ, that is the non-trivial one dimensional irreducible lifted from $\mathbb{Z}_2[D_{2p}/C_p]$, is one such module.

When $\ell = p$, the Yakovlev diagram of a $\mathbb{Z}_p[G]$-lattice M consists of $H^1(C_p, M)$ as a $\mathbb{F}_p[D_{2p}/C_p]$-module. Since $\text{char}(\mathbb{F}_p) \neq 2$, there are two irreducible $\mathbb{F}_p[D_{2p}/C_p]$-modules, both one dimensional, one with trivial action and one without. So any two lattices whose cohomology exhibits these modules will extend S to a basis of $A(\mathbb{Z}_p[G])$. If ρ denotes the $(p-1)$-dimensional irreducible $\mathbb{Q}_p[G]$-representation, then there are two non-isomorphic $\mathbb{Z}_p[G]$-sublattices A, A' contained in ρ, with $H^1(C_p, A), H^1(C_p, A') \cong \mathbb{Z}/p\mathbb{Z}$ as abelian groups, but the former having non-trivial D_{2p}/C_p action and D_{2p}/C_p acting trivially on the latter. These modules are explicitly constructed in [Lee64].

In conclusion,

$$\dim_\mathbb{Q}(A(\mathbb{Z}_\ell[G])) = \begin{cases} 3 & \ell \neq 2, p \\ 4 & \ell = 2 \\ 6 & \ell = p \end{cases}.$$

with a basis S' given by

$$S' = \begin{cases} \mathbb{1}_{\{1\}}\uparrow^G, \mathbb{1}_{C_2}\uparrow^G, \mathbb{1}_{C_p}\uparrow^G & \ell \neq 2, p \\ \mathbb{1}_{\{1\}}\uparrow^G, \mathbb{1}_{C_2}\uparrow^G, \mathbb{1}_{C_p}\uparrow^G, \epsilon & \ell = 2 \\ \mathbb{1}_{\{1\}}\uparrow^G, \mathbb{1}_{C_2}\uparrow^G, \mathbb{1}_{C_p}\uparrow^G, \mathbb{1}_G, A, A' & \ell = p \end{cases} .$$

Denote the extension of scalars map $A(\mathbb{Z}_\ell[G]) \to A(\mathbb{Q}_\ell[G])$ by a, and the map $A(\mathbb{Z}_\ell[G]) \to \bigoplus_{H\in\mathrm{nchyp}_\ell(G)} \mathbb{Q}$ which assigns a lattice M the vector $(v_p(C_{\theta_H}(M)))_{H\in\mathrm{nchyp}_\ell(G)}$ by b. Then, Theorem 6.8 states that $a \oplus b \oplus \mathrm{Yak}$ is injective (and so an isomorphism). The matrix representing $a \oplus b \oplus \mathrm{Yak}$ is given by:

$$\begin{array}{c} \\ \mathbb{1} \\ \epsilon \\ \rho \end{array} \begin{array}{ccc} \mathbb{1}\uparrow^G_{\{1\}} & \mathbb{1}\uparrow^G_{C_2} & \mathbb{1}\uparrow^G_{C_p} \\ \left(\begin{array}{ccc} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{array} \right) \end{array} \qquad \text{if } \ell \neq 2, p \,,$$

$$\begin{array}{c} \\ \mathbb{1} \\ \epsilon \\ \rho \\ \mathrm{Yak}(-) \end{array} \begin{array}{cccc} \mathbb{1}\uparrow^G_{\{1\}} & \mathbb{1}\uparrow^G_{C_2} & \mathbb{1}\uparrow^G_{C_p} & \epsilon \\ \left(\begin{array}{ccc|c} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right) \end{array} \qquad \text{if } \ell = 2,$$

$$\begin{array}{c} \\ \mathbb{1} \\ \epsilon \\ \rho \\ v_p(C_{\theta_G}(-)) \\ \\ \mathrm{Yak}(-) \end{array} \begin{array}{cccccc} \mathbb{1}\uparrow^G_{\{1\}} & \mathbb{1}\uparrow^G_{C_2} & \mathbb{1}\uparrow^G_{C_p} & \mathbb{1}_G & A & A' \\ \left(\begin{array}{ccc|c|cc} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & -1/2 & 1/2 & -1/2 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right) \end{array} \qquad \text{if } \ell = p.$$

Here, we take the basis $\mathbb{1}, \epsilon, \rho$ of $\mathbb{Q}_\ell[G]$, where $\mathbb{1}, \epsilon$ are the trivial and non-trivial one dimensional irreducibles and ρ the $(p-1)$ dimensional irreducible. When $\ell = 2$, the basis of $\mathcal{C}$ is taken to be $\mathbb{Z}/2\mathbb{Z}$, and when $\ell = p$, the basis is given by $\mathbb{Z}/p\mathbb{Z}$ with both its non-trivial and trivial $C_2 \cong D_{2p}/C_p$-actions respectively. The calculations of $v_p(C_{\theta_G}(A)), v_p(C_\theta(A'))$ can be found in [Bar12, Thm. 4.4].

REMARK 7.1 For $p \leq 67$, a $\mathbb{Z}[D_{2p}]$-lattice is determined by its localisation at the primes $2, p$ (see [Bar12, Ex. 6.3]). So, by applying Theorem 6.8 at both primes we obtain a finite list of data which specifies the isomorphism class of an arbitrary $\mathbb{Z}[D_{2p}]$-lattice.

REMARK 7.2 The above matrices can be seen to be block upper triangular. This was touched on in the proof of Lemma 3.17 and is a general phenomenon.

7.2   Groups with degenerate permutation pairing

EXAMPLE 7.3 Let $G = C_3 \times C_3 \times S_3$, a 3-hypo-elementary group. Up to conjugacy G has 17 subgroups, but the permutation pairing of Construction 3.8 is degenerate and has rank 16.

In this section, we define a canonical Brauer relation $\theta_{\Sigma,G}$ which is non-zero for any non-cyclic group G. When $G = C_3 \times C_3 \times S_3$, then $\theta_{\Sigma,G}$ generates the kernel of the permutation pairing.

NOTATION 7.4   • Let G be any finite group and Σ denote the set of all subgroups of G, which is partially ordered with respect to containment. Let $\mu_\Sigma \colon \Sigma \to \mathbb{Z}$ denote the Möbius function on Σ, i.e. the unique function for which

$$\mu_\Sigma(G) = 1$$

and

$$\sum_{H' \geq H} \mu_\Sigma(H') = 0$$

for all $H \neq G$.

• Set

$$\theta_{\Sigma,G} = \sum_{H \in \Sigma} \frac{\mu_\Sigma(H)}{|G : H|}[H] \in B(G).$$

• For an element $\theta \in B(G)$ and $K \leq G$, let θ^K denote the number of fixed points of θ under K, i.e. if $\theta = \sum_H \alpha_H[H]$ then $\theta^K = \sum \alpha_H \#([H]^K)$.

LEMMA 7.5 *For any $K \leq G$, $(\theta_{\Sigma,G})^K = \sum_{H \geq K} \mu_\Sigma(H)$.*

Proof. Since both $\#[H]^K$ and $\mu_\Sigma(H)$ are constant under replacing H with a conjugate, we have

$$\sum_{H \leq G} \frac{\mu_\Sigma(H)}{|G : H|} \#([H]^K) = \sum_{H \leq_G G} \frac{|H|\mu_\Sigma(H)}{|N_G(H)|} \#([H]^K)$$

$$= \sum_{H \leq_G G} \frac{|H|\mu_\Sigma(H)}{|N_G(H)|} |\{g \in G/H \mid K^g \leq H\}|$$

$$= \sum_{H \leq_G G} \frac{|H|\mu_\Sigma(H)}{|N_G(H)|} |\{g \in G/H \mid K \leq H^g\}|$$

$$= \sum_{H \leq_G G} \frac{|H|\mu_\Sigma(H)}{|N_G(H)|} \cdot \frac{|N_G(H)|}{|H|} |\{g \in G/N_G(H) \mid K \leq H^g\}|$$

$$= \sum_{H \geq K} \mu_\Sigma(H).$$

$\square$

COROLLARY 7.6 *For any finite group G,*

  i) $\theta_{\Sigma,G}$ *is a Brauer relation in characteristic zero if and only if G is non-cyclic,*

 ii) $\theta_{\Sigma,G}$ *is a Brauer relation in characteristic p if and only if G is non-p-hypo-elementary,*

iii) $\theta_{\Sigma,G}\!\downarrow_H$ *is zero for all proper subgroups H.*

Proof. We first check *i)*. An element of $B(G)$ is a relation in characteristic zero if and only if the number of its fixed points under all cyclic subgroups is zero (see for example the proof of [Ben98, Thm. 5.6.1]). By the lemma, $\theta_{\Sigma,G}$ is a relation in characteristic zero if and only if

$$\sum_{H \geq C} \mu_\Sigma(H) = 0$$

for all cyclic subgroups C. By the definition of μ_Σ, this is true if and only if G is not itself cyclic.

The argument for *ii)* is identical instead using that elements of $B(G)$ are relations in characteristic p if and only if the number of fixed points under all p-hypo-elementary subgroups is zero (repeat the proof of [Ben98, Thm. 5.6.1] but using species and Lemma 6.18).

For *iii)*, simply note that an element of $B(H)$ is zero if and only if its fixed points under all subgroups is zero (proven analogously to the previous cases). But $(\theta_{\Sigma,G}{\downarrow}_H)^K = (\theta_{\Sigma,G})^K$, which by the lemma vanishes for all proper subgroups $K < G$. □

REMARK 7.7 By Lemma 2.27 *iv)*, $\theta_{\Sigma,G}$ automatically vanishes on all permutation modules other than possibly the trivial representation. In Example 7.3, $C_3 \times C_3 \times S_3$ is a group for which in addition $\theta_{\Sigma,G}(\mathbb{1}_G) = 1$.

EXAMPLE 7.8 Let $G = (C_p \times C_p) \rtimes C_q$ with p, q odd primes and $p = 2q + 1$ and where C_q acts diagonally on $C_p \times C_p$. Write $\alpha_H = \mu_\Sigma(H)/|G : H|$ so that $\theta_{\Sigma,G} = \sum_{H \leq G} \alpha_H[H]$. Then, the α_H for each conjugacy class are given in the following table:

	1	C_q	C_p	C_p	C_p	C_p	$C_p \rtimes C_q$	$C_p \rtimes C_q$	$C_p \times C_p$	G
#conjugates	1	p^2	1	1	q	q	p	p	1	1
$\mu_\Sigma(H)$	$-p^2$	1	p	p	0	0	-1	-1	-1	1
α_H	$-1/q$	$1/p^2$	$1/q$	$1/q$	0	0	$-1/p$	$-1/p$	$-1/q$	1

And we find $\theta_{\Sigma,G}(\mathbb{1}_G) = 1$. Thus, the relation $\theta_{\Sigma,G}$ is trivial on all permutation representations. As G is p-hypo-elementary, $\theta_{\Sigma,G}$ is not a p-relation and the permutation pairing of Construction 3.8 is degenerate.

REMARK 7.9 It is not clear to the author if, for any of the above groups, there exists a lattice M for which $\theta_{\Sigma,G}(M) \neq 1$. Necessarily, such an M must not be induced from a proper subgroup (Lemma 2.27). For $G = C_3 \times C_3 \times S_3$, $A(\mathbb{Z}_3[G], \mathrm{perm}) = A(\mathbb{Z}_{(3)}[G], \mathrm{triv}) = A(\mathbb{Z}_3[G], \mathrm{triv})$ since G has the same number of species as conjugacy classes of p-hypo-elementary subgroups (Lemma 6.25 *iv)*). Thus, such an M would also have to not have trivial source.

References

[Bar12] A. Bartel, *On Brauer-Kuroda type relations of S-class numbers in dihedral extensions*, J. Reine Angew. Math. **668** (2012), 211–244.

[BD14] A. Bartel and T. Dokchitser, *Brauer relations in finite groups II: Quasi-elementary groups of order $p^a q$*, J. Group Theory **17** (2014), no. 3, 381–393.

[BD15] ―――, *Brauer relations in finite groups*, J. Eur. Math. Soc. (JEMS) **17** (2015), no. 10, 2473–2512.

[Beg10] A. Bege, *Generalized GCD matrices*, Acta Univ. Sapientiae Math. **2** (2010), no. 2, 160–167.

[Ben98] D. J. Benson, *Representations and cohomology. I,* second ed., Cambridge Studies in Advanced Mathematics, vol. 30, Cambridge University Press, Cambridge, 1998, Basic representation theory of finite groups and associative algebras.

[Ben06] E. Beneish, *Failure of Krull-Schmidt for invertible lattices over a discrete valuation ring,* Proc. Amer. Math. Soc. **134** (2006), no. 7, 1869–1873.

[BL89] S. Beslin and S. Ligh, *Greatest common divisor matrices,* Linear Algebra Appl. **118** (1989), 69–76.

[CR94] C. W. Curtis and I. Reiner, *Methods of Representation Theory Volume I,* Wiley, 1994.

[DD09] T. Dokchitser and V. Dokchitser, *Regulator constants and the parity conjecture,* Invent. Math. **178** (2009), no. 1, 23–71.

[Fan91] Y. Fan, *Permutation modules, p-permutation modules and Conlon species,* Sci. China Ser. A **34** (1991), no. 11, 1290–1301.

[HR62] A. Heller and I. Reiner, *Representations of cyclic groups in rings of integers. I,* Ann. of Math. (2) **76** (1962), 73–92.

[Lee64] M. P. Lee, *Integral representations of dihedral groups of order $2p$,* Trans. Amer. Math. Soc. **110** (1964), 213–231.

[Rei70] I. Reiner, *A survey of integral representation theory,* Bull. Amer. Math. Soc. **76** (1970), 159–227.

[Sna94] V. P. Snaith, *Explicit Brauer induction,* Cambridge Studies in Advanced Mathematics, vol. 40, Cambridge University Press, Cambridge, 1994, With applications to algebra and number theory.

[Tor18] A. Torzewski, *Regulator constants of integral representations, together with relative motives over shimura varieties,* Ph.D. thesis, University of Warwick, July 2018.

[Yak96] A. V. Yakovlev, *Homological definability of p-adic representations of groups with cyclic Sylow p-subgroup,* An. Ştiinţ. Univ. Ovidius Constanţa Ser. Mat. **4** (1996), no. 2, 206–221, Representation theory of groups, algebras, and orders (Constanţa, 1995).

MATHEMATICS INSTITUTE, ZEEMAN BUILDING, UNIVERSITY OF WARWICK, COVENTRY CV4 7AL, UK

E-mail address: `alex.torzewski@gmail.com`